PREVENTION OF AND RESPONSE TO THE ARRIVAL OF A DIRTY BOMB AT A U.S. PORT

(114–30)

HEARING

BEFORE THE

SUBCOMMITTEE ON
COAST GUARD AND MARITIME TRANSPORTATION

OF THE

COMMITTEE ON
TRANSPORTATION AND
INFRASTRUCTURE
HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

OCTOBER 27, 2015

Printed for the use of the
Committee on Transportation and Infrastructure

Available online at: http://www.gpo.gov/fdsys/browse/committee.action?chamber=house&committee=transportation

U.S. GOVERNMENT PUBLISHING OFFICE

97–310 PDF WASHINGTON : 2016

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE

BILL SHUSTER, Pennsylvania, *Chairman*

DON YOUNG, Alaska
JOHN J. DUNCAN, JR., Tennessee, *Vice Chair*
JOHN L. MICA, Florida
FRANK A. LOBIONDO, New Jersey
SAM GRAVES, Missouri
CANDICE S. MILLER, Michigan
DUNCAN HUNTER, California
ERIC A. "RICK" CRAWFORD, Arkansas
LOU BARLETTA, Pennsylvania
BLAKE FARENTHOLD, Texas
BOB GIBBS, Ohio
RICHARD L. HANNA, New York
DANIEL WEBSTER, Florida
JEFF DENHAM, California
REID J. RIBBLE, Wisconsin
THOMAS MASSIE, Kentucky
TOM RICE, South Carolina
MARK MEADOWS, North Carolina
SCOTT PERRY, Pennsylvania
RODNEY DAVIS, Illinois
MARK SANFORD, South Carolina
ROB WOODALL, Georgia
TODD ROKITA, Indiana
JOHN KATKO, New York
BRIAN BABIN, Texas
CRESENT HARDY, Nevada
RYAN A. COSTELLO, Pennsylvania
GARRET GRAVES, Louisiana
MIMI WALTERS, California
BARBARA COMSTOCK, Virginia
CARLOS CURBELO, Florida
DAVID ROUZER, North Carolina
LEE M. ZELDIN, New York
PETER A. DEFAZIO, Oregon
ELEANOR HOLMES NORTON, District of Columbia
JERROLD NADLER, New York
CORRINE BROWN, Florida
EDDIE BERNICE JOHNSON, Texas
ELIJAH E. CUMMINGS, Maryland
RICK LARSEN, Washington
MICHAEL E. CAPUANO, Massachusetts
GRACE F. NAPOLITANO, California
DANIEL LIPINSKI, Illinois
STEVE COHEN, Tennessee
ALBIO SIRES, New Jersey
DONNA F. EDWARDS, Maryland
JOHN GARAMENDI, California
ANDRÉ CARSON, Indiana
JANICE HAHN, California
RICHARD M. NOLAN, Minnesota
ANN KIRKPATRICK, Arizona
DINA TITUS, Nevada
SEAN PATRICK MALONEY, New York
ELIZABETH H. ESTY, Connecticut
LOIS FRANKEL, Florida
CHERI BUSTOS, Illinois
JARED HUFFMAN, California
JULIA BROWNLEY, California

SUBCOMMITTEE ON COAST GUARD AND MARITIME TRANSPORTATION

DUNCAN HUNTER, California, *Chairman*

DON YOUNG, Alaska
FRANK A. LOBIONDO, New Jersey
BOB GIBBS, Ohio
MARK SANFORD, South Carolina
GARRET GRAVES, Louisiana
CARLOS CURBELO, Florida
DAVID ROUZER, North Carolina
LEE M. ZELDIN, New York
BILL SHUSTER, Pennsylvania *(Ex Officio)*
JOHN GARAMENDI, California
ELIJAH E. CUMMINGS, Maryland
CORRINE BROWN, Florida
JANICE HAHN, California
LOIS FRANKEL, Florida
JULIA BROWNLEY, California
PETER A. DEFAZIO, Oregon *(Ex Officio)*

CONTENTS

Committee on Transportation and Infrastructure
U.S. House of Representatives
Washington, DC 20515

Bill Shuster
Chairman

Peter A. DeFazio
Ranking Member

Christopher P. Bertram, Staff Director

Katherine W. Dedrick, Democratic Staff Director

October 23, 2015

SUMMARY OF SUBJECT MATTER

TO: Members, Subcommittee on Coast Guard and Maritime Transportation
FROM: Staff, Subcommittee on Coast Guard and Maritime Transportation
RE: Coast Guard hearing on "The Prevention of and Response to the Arrival of a Dirty Bomb at a U.S. Port"

PURPOSE

On October 27, 2015, at 10:00 a.m., in 2167 Rayburn House Office Building, the Subcommittee on Coast Guard and Maritime Transportation will hold a hearing on the Prevention of and Response to the Arrival of a Dirty Bomb at a U.S. Port. The Subcommittee will hear from the U.S. Coast Guard, the Domestic Nuclear Detection Office, U.S. Customs and Border Protection, the U.S. Government Accountability Office, Sandia National Laboratories, Los Alamos National Laboratory, the American Association of Port Authorities, and the George J. Kostas Research Institute for Homeland Security.

BACKGROUND

The U.S. maritime border includes 95,000 miles of open shoreline, 361 ports and an Exclusive Economic Zone that spans 3.5 million square miles. These ports connect to 152,000 miles of railways, 460,000 miles of underground pipelines and 45,000 miles of interstate highways. The U.S. relies on ocean transportation for 95 percent of cargo tonnage that moves in and out of the country. U.S. Department of Transportation data shows 7,836 commercial vessels made 68,036 port calls in 2011. According to U.S. Customs and Border Protection (CBP), in 2014, 11 million shipping containers arrived on ships and entered U.S. seaports, representing nearly half of incoming U.S. trade (by value).

Standard sizes of shipping containers allow cargo to be quickly transferred from ships to trucks or railcars and transported efficiently to anywhere in the country. This rapid transfer of cargo has been viewed as a possible conduit and target for terrorist activities. The Department of Homeland Security (DHS) reported in 2009 that the likelihood of a terrorist smuggling weapons of mass destruction into the U.S. in shipping containers is low, the Nation's vulnerability to this

activity and consequences of such an attack – revenue losses, loss of lives, and disruption in manufacturing and other economic activities – are potentially high.

A "dirty bomb" is a type of radiological dispersal device (RDD) that combines conventional explosives, such as dynamite, with radioactive material. According to the U.S. Nuclear Regulatory Commission, an RDD would not release enough radiation to kill people or cause severe illness. The explosion from the conventional explosives used in the bomb would be more harmful to anyone near the event than the radioactive material. However, it is acknowledged that the use of an RDD is likely to create fear and panic, contaminate property, require a potentially costly cleanup, and if it occurred at a U.S. port, a shutdown of that port.

Radioisotopes, such as cobalt-60 and cesium-137, which can be used to construct an RDD, are fairly common radioactive elements with each having legitimate medical, commercial and industrial uses. Organizations such as the International Atomic Energy Agency warn that such radioisotopes are readily available to virtually any country in the world; moreover they are almost certainly not beyond the reach of even moderately capable non-state actors.

On October 7, 2015, the Associated Press reported that the Federal Bureau of Investigations (FBI), working with Eastern European authorities, over the last five years interrupted four attempts by criminal gangs with suspected Russian connections to sell radioactive material (cesium) to Middle Eastern extremists. The most recent attempt was in February 2015, in the Eastern European country of Moldova, where the sale was interrupted by authorities. This successful disruption showed that intelligence efforts to monitor movement of unregulated radioactive materials are working. Authorities stress the need to maintain these monitoring initiatives to deter or thwart this illegal trade in the future.

Prior to September 11, 2001, the primary focus of intermodal transportation was the safe movement of shipping containers in a timely manner. As a result of ongoing terrorist threats, the U.S. continues to develop and improve its security regime to minimize the risks and consequences of a terrorist attack without slowing the movement of cargo.

Legislation enacted after 9/11 includes:

- The Trade Act of 2002 (P.L. 107-210) requires importers and exporters to submit cargo manifest data 24 hours in advance of cargo arriving at a U.S. port.

- The Maritime Transportation and Security Act of 2002 (MTSA) (P.L. 107-295), now Chapter 701 of title 46, Port Security, established DHS's overall role in the port security regime. It required DHS to review vessel and port security and develop regional and national maritime transportation security plans. It also created the Transportation Worker Identity Credential (TWIC) cards administered by the Transportation Security Administration (TSA) and the U.S. Coast Guard (Coast Guard). MTSA requires DHS to assess foreign port security measures and if a foreign port fails to maintain certain security standards, DHS can prohibit vessels coming from those foreign ports access to U.S. ports.

- The Security and Accountability for Every (SAFE) Port Act of 2006 (P.L. 1090-347) (6 U.S.C. 901 et. seq.) made adjustments to the MTSA and codified authorities for the Customs-Trade Partnership Against Terrorism, the Container Security Initiative, and the Domestic Nuclear Detection Office.

- The Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act) (P.L. 110-53) amended the SAFE Port Act to require by July 2012, 100 percent of all U.S. bound shipping containers be scanned at foreign ports with both radiation-detection and nonintrusive inspection equipment before being placed on U.S.-bound vessels. The law allowed DHS to grant extensions to ports that cannot support 100 percent scanning.

Efforts to secure the supply chain

DHS uses a multilayered and risk based security approach that extends beyond the domestic border and ports. Several agencies within the DHS are involved in monitoring threats to the U.S. global supply chain and the movement of goods and materials into and out of the U.S. According to DHS its security measures take place at different locations, at different times, and by different organizations based on their jurisdiction.

CBP has primary federal responsibility to ensure that all imports and exports comply with U.S. laws and regulations. CBP works to balance the three overarching U.S. import policies: 1) trade facilitation; 2) enforcement of trade laws; and 3) import security. CBP initiatives focus on the goal of checking the security of cargo before it reaches the U.S.

The U.S. Coast Guard (USCG) has primary responsibility for the protection of life and property at sea, as well as the enforcement of all applicable federal laws on, under, and over the highs seas and U.S. waters. The USCG also coordinates all maritime security planning and is responsible for the security of U.S. ports, harbors, waterways, vessels and waterfront facilities.

The Government Accountability Office (GAO) 2010 report entitled *Maritime Security DHS Progress and Challenges in Key Areas of Port Security* notes DHS and its agencies have strengthened risk management decisions through continually evolving risk assessment tools. DHS and CBP have taken various actions to enhance maritime container security. The USCG has initiated similar actions for port security.

The USCG transitioned in 2005 from its Port Security Risk Assessment Tool (PS-RAT) to Maritime Security Risk Assessment Model (MSRAM). PS-RAT had allowed ports to prioritize resource allocation within a port, but not between ports. MSRAM allows port risk assessments across multiple ports, where USCG units assess risks-threats, vulnerabilities, and consequences-of a terrorist attack using different scenarios and targets and then applies MSRAM information to direct the allocation of USCG resources as needed to U.S. ports.

The USCG requires all vessels to provide notice of arrival (NOA) to any U.S. port 96 hours in advance, an increase from the previous NOA requirement of 24 hours. In addition, the notice must now include a listing of all persons on board, crew and passengers, with date of birth, nationality, along with the appropriate passport or mariner's document number. The notice

must also include the vessel name, country of registry, call sign, official number, the registered owner of the vessel, the operator, the name of the classification society, a general description of the cargo, and the date of departure from the last port along with that port's name.

The USCG uses the International Maritime Organization's (IMO) International Ship and Port Facility Security (ISPS) Code in its International Port Security Program. The ISPS Code is a global bench mark that measures the effectiveness of a country's counterterrorism measures at a port. USCG personnel visit foreign ports to determine compliance with ISPS. However, the 2010 GAO report states that some countries have been reluctant to allow the USCG to conduct visits at their ports due to concerns over sovereignty. Reciprocal arrangements and visits between the USCG and foreign trade partners have helped gain cooperation. Vessels subject to ISPS Code must maintain their security systems not only in port, but also in transit.

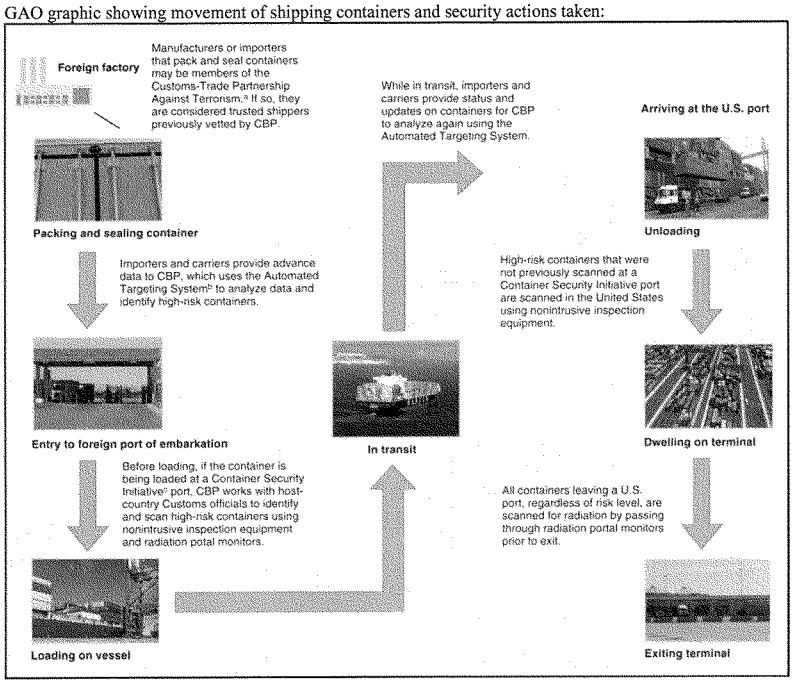
Per the Trade Act of 2002 (P.L. 107-210), cargo container manifests are required to be submitted to CBP 24 hours before shipping containers are loaded at a foreign port onto a U.S.-bound vessel. Other information collected by CBP, per the SAFE Port Act, is commonly referred to as "10+2" shipper information. This information includes ten elements provided from importers (importer record number, consignee number, seller name and address, buyer name and address, ship-to party name and address, manufacturer name and address, country of origin, Harmonized Tariff Schedule, container location, consolidator (stuffer) name and address) and two elements provided from ocean carriers (vessel stow plan and daily messages with information about container status changes). All of this data is sent to the CBP National Targeting Center – Cargo (NTC-C) in Herndon, VA. CBP uses the data to conducts risk-based targeting through its Automated Targeting System (ATS) which is a mathematical model that uses weighted rules and algorithms to assign a risk score to arriving cargo shipments. ATS is a decision support tool the CBP uses to compare traveler, cargo, and conveyance information against law enforcement intelligence and other data. Using this method, NTC-C screens 100 percent of shipping container and vessel manifest data to determine what shipping containers are high-risk.

CBP runs two voluntary programs – the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT) – which were codified in the SAFE Port Act (6 U.S.C. 961). Under C-TPAT, partnerships are established with importers, carriers, brokers, warehouse operators and manufacturers to improve security along the entire supply chain. CBP, along with its C-TPAT partners, examine where cargo originate and assess the physical security and integrity of the foreign suppliers, the background of the personnel involved with the transaction, and the means by which goods are transported to the U.S. As of September 2014, C-TPAT had 10,834 program participants. In June 2014, C-TPAT officials signed a mutual recognition arrangement with Israel's Authorized Economic Operator (AEO) program to further secure and facilitate global cargo trade and allow members of the two programs fewer cargo exams and a faster validation process. The U.S. has similar C-TPAT arrangements with New Zealand, Canada, Japan, Korea, Jordan, the European Union, and Taiwan and is working on C-TPAT arrangements with Mexico, China, India, and Brazil.

The goal of the CSI is to reduce the vulnerability of shipping containers being used to smuggle terrorists or terrorist weapons while accommodating the need for efficiency in global commerce. CBP initially focused implementation of CSI at the 60 largest foreign seaports

responsible for shipping the greatest number of shipping containers to the U.S. which carry approximately 80 percent of all U.S. incoming containerized cargo. CBP reports NTC-C provides targeting support for these 60 overseas CSI locations. In cooperation with the host countries, CBP reported in 2013 that it reviewed 11,228,203 bills of lading and conducted 103,999 examinations of high-risk cargo.

GAO graphic showing movement of shipping containers and security actions taken:



Source: GAO (analysis); GAO and DHS S&T (photos) and Art Explosion (clipart).

The World Customs Organization (WCO) is the only international body dedicated exclusively to international customs and border control matters. CBP is the lead U.S. agency engaged with the WCO. CBP works with the WCO to integrate domestic measures including "10+2" data elements into international security standards.

If an NTC-C review of shipping container manifest data indicates a high-risk container, CBP will work with staff at CSI ports to get the high risk container scanned. Primary scanning is accomplished through the use of non-intrusive inspections (NII) which involve 1) large-scale X-ray and gamma ray imaging systems, and 2) Radiation Portal Monitor (RPM) for radiation. If the NII measures cannot resolve the issue, a physical inspection of the container will then occur. NTC-C staff also reviews manifest data for containers starting from non-CSI ports. NTC-C staff

will coordinate with U.S. State Department and local port authorities to get non-intrusive scanning or physical inspections for any identified high-risk containers.

CBP uses non-intrusive technology for cargo entering and leaving U.S. ports. Radiation Portal Monitors (RPMs), installed by the DHS, DNDO and CBP, are capable of detecting radiation emanating from nuclear devices, dirty bombs, special nuclear materials, natural sources and isotopes commonly used in medicine and industry. "Portal technology" can detect even the weakest radiation and then use sophisticated computer software to specifically identify the source. Any cargo container that triggers an alarm is set aside for more scanning or inspections. Radiological readings are sent to Laboratories and Scientific Services when further adjudication (the process to identify the type or nature of the material and assess the potential threat) is needed. CBP officers also carry radiation isotope identification devices (RIID) which can identify the radiation source, which can include some of the following materials plutonium, kitty litter and granite.

CBP's 2014 Performance and Accountability Report notes that by the end of FY 2014, CBP deployed NII technologies to air, land, and sea ports of entry and to Border Patrol checkpoints including 314 large-scale imaging systems, 1,362 radiation portal monitors, 2,979 radiation isotope identification devices, and 30,305 personal radiation detectors. In 2014, CBP used these large-scale systems in more than 7.2 million examinations, resulting in more than 2,093 seizures and the interception of more than 249,200 pounds of narcotics. CBP says the technology provides a non-intrusive means to scan 100 percent of vehicles and shipping containers for radiation entering the country while facilitating the flow of legitimate travel and trade. CBP also states that 99 percent of all incoming containerized cargo arriving in the U.S. by sea is processed through an RPM.

In addition, the Border Security Deployment Program has an integrated surveillance and intrusion - detection system consisting of more than 8,400 cameras and microphones—that provide security, motion detection, and remote monitoring capabilities across every U.S. land port of entry. The system connects via the DHS Wide Area Network to remote monitoring stations called Customs Area Security Centers. These centralized command centers house digital video recorders augmented with analytic software to alert watch officers of a detected alarm or intrusion within a port facility and archive the event as evidence in subsequent investigations and prosecutions.

The SAFE Port Act (6 U.S.C. 981) required DHS to implement a Secure Freight Initiative (SFI) using non-intrusive imaging equipment and radiation detection equipment to scan shipping containers. DHS implemented the pilot project in 2007 at three international ports – Qasim in Pakistan, Puerto Cortes in Honduras, and Southhampton in United Kingdom. It was extended on a limited basis to the ports of Salalah in Oman, Busan in South Korea, and in Singapore. SFI was scaled back due to a number of issues, including lack of host state support and costs. CBP reported the cost of SFI pilot project was about $120 million over the first three years. In 2015, only the Port of Qasim in Pakistan is still operational.

The SAFE Port Act (6 U.S.C. 982), as amended by the 9/11 Commission Act, required 100 percent scanning of U.S.-bound shipping containers by 2012. GAO noted in its June 22, 2015, report entitled *U.S. Customs and Border Protection: Trade Facilitation, Enforcement, and*

Security that 100 percent scanning had not been achieved and the feasibility of 100 percent scanning remained unproven. The June 2015 GAO report referred to a 2012 CBO estimate which determined that implementation of 100 percent scanning would cost an average of $8 million per shipping lane and total $16.8 billion for all U.S.-bound containers. GAO also noted that most NII scanning of shipping containers occurs in U.S. ports, not at foreign ports.

The SAFE Port Act (6 U.S.C. 982), as amended by the 9/11 Commission Act, also authorized the DHS Secretary to issue two-year extensions for foreign ports that could not meet the 100 percent scanning requirement. In May 2012, then-DHS Secretary Janet Napolitano issued a blanket two-year extension for all foreign ports; DHS Secretary Jeh Johnson subsequently issued another two-year extension in May 2014. Secretary Johnson noted in his letter to Congress regarding the extension, that DHS's ability to fully comply with 100 percent scanning is highly improbable. The Congressional Research Service March 20, 2015, report entitled *Transportation Security: Issues for the 114th Congress* mentions that U.S. trading partners do not support 100 percent scanning. It also noted a European Commission (EC) determination that 100 percent scanning is the wrong approach and that the EC supports a multilayered risk management approach.

Efforts to deter, detect, and respond to smuggling activities

The DNDO has a mission to counter the risk of nuclear terrorism in the U.S. by continuously improving capabilities to deter, detect, respond to, and attribute attacks, in coordination with domestic (federal agencies, state, tribal, and local governments) and international (foreign governments) partners. DNDO works with federal partners – Departments of Defense, Energy, Justice, and State, the Intelligence Community and the Nuclear Regulatory Commission – to develop the Global Nuclear Domestic Architecture (GNDA). DNDO implements the GNDA domestic component to detect and interdict nuclear smuggling. GNDA is a multi-layered, world-wide network that combines 74 independent federal programs, projects, or activities to detect and interdict nuclear smuggling in foreign countries, at the U.S. border, and within the U.S. It includes sensors, telecommunications, and personnel, along with supporting information exchanges, programs, and protocols, that serve collectively to detect, analyze, and report on nuclear and radiological materials that are out of regulatory control.

DNDO works with its federal and non-federal partners to determine gaps in the GNDA and implements coordinated research programs to develop technologies and protocols to address those gaps. End users of the technologies developed include CBP, USCG, Transportation Security Administration, state, local, and tribal law enforcement agencies.

DNDO is made up of seven Directorates. These directorates focus on the following activities:

- determining gaps or vulnerabilities in the GNDA
- conducting engineering development and deployment of technologies
- coordinating long-term research and development
- developing information sharing and analytical tools
- ensuring that DNDO proposes sound technical solutions and understands system performance and vulnerabilities

- providing national-level stewardship procedures, protocols, centralized planning and integration for nuclear forensics.

DNDO's Transformational and Applied Research (TAR) Directorate determines what research initiatives to prioritize and fund. During fiscal years 2008-2013, DNDO obligated roughly $350 million for 189 research and development projects, of which approximately $103 million went to 48 projects focused on detecting shielded nuclear material.

GAO, in its March 2015 report entitled *Combating Nuclear Smuggling – DHS Research and Development on Radiation Detection Technology Could Be Strengthened* reviewed DNDO research programs and their ability to meet GNDA needs. GAO's performance audit ran from November 2013 to March 2015. GAO found that DNDO's TAR Directorate did not have documentation showing how its research and developed technologies resolve identified gaps in the GNDA. GAO recommended DNDO's TAR Directorate develop a research road map and implementation strategy to guide research. TAR should also better document how it prioritizes research, and it should develop a way to evaluate how research and development projects meet the TAR Directorate's overall research challenges (i.e. address gaps in the GNDA).

The September 2014 GAO (unclassified) report entitled *Combating Nuclear Smuggling – Risk-Informed Covert Assessment and Oversight of Corrective Actions Could Strengthen Capabilities at the Border* found that over the period of 2006 through 2013 CBP's Operational Field Testing Division (OFTD) conducted 144 covert operations at 86 locations out of 665 U.S. air, land, and sea port facilities; checkpoints; and certain international locations. These OFTD covert operations allow CBP to assess capabilities and procedures to detect and interdict or intercept nuclear and radiological materials at the 86 locations. GAO noted that while OFTD issues reports (although, not on a timely basis) that include recommendations for corrective actions, CBP does not track corrective actions taken to address areas of concern. GAO recommended creating a tracking mechanism to account for corrective measures taken at ports of entry and check points to assist in directing where resource investments (equipment and personnel training) should be made to assist CBP in deterring smuggling efforts.

A covert operation was considered successful, if a CBP officer or U.S. Border Protection agent both detected and interdicted the test source using standard operating procedures. GAO redacted the results of the 38 tests for security purposes. GAO noted in the report that CBP has not conducted risk assessments that could be incorporated into the decision making process for prioritizing materials, locations, and technologies tested in the covert operations and references a DHS 2010 Policy for Integrated Risk Management that says its components should use such assessments. CBP's 2013 Integrated Planning Guidance for fiscal years 2015 through 2019 included recommendations for integrating risk assessments into decision making, but CBP has not yet taken this step. GAO recommended in its report that the Secretary of Homeland Security conduct or use a risk assessment to inform department priorities and to assist CBP in getting information necessary for oversight and accountability – determine timeframes for OFTD reporting, and develop mechanisms to track corrective actions.

Maritime Domain Awareness

The 2013 *National Maritime Domain Awareness Plan for The National Strategy for Maritime Security* (2013 Plan) defines "Maritime Domain" as all areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean or other navigable waterway, including all maritime-related activities, infrastructure, people cargo, vessels and other conveyances. "Maritime Domain Awareness" is defined in the 2013 Plan as the effective understanding of anything associated with the maritime domain that could impact the security, safety, economy, or environment of the U.S.

The FBI, DHS and DOD share responsibility to keep threats from entering the U.S.; however, should an event occur inside the U.S., the USCG and DHS support the FBI's lead for law enforcement. The Maritime Operational Threat Response (MOTR) facilitates interagency coordination for situations requiring multiple agencies coordination. The final MOTR plan was signed in 2006 and is the presidentially approved plan to achieve a coordinated U.S. government response to threats in the maritime domain. The Global MOTR Coordination Center was established in 2010 and includes the Departments of State, Defense, Justice, Commerce, Transportation, and Homeland Security.

Federal law authorizes the USCG to board any vessel subject to the jurisdiction, or operation of any law, of the U.S. in order to make inquiries, examinations, inspections, searches, seizures, and arrests for the violations of U.S. laws. The USCG may order and force any vessel to stop and may engage in land, water, and air patrols. Federal law also authorizes the USCG to control the anchorage and movement of vessels in the navigable waters of the U.S. Each USCG Captain of the Port may employ any additional security measures that he deems necessary to ensure the safety and security of the port, including prohibiting a vessel from entering the port. Per DHS, all USCG vessel boarding and inspection teams are equipped with nuclear/radiological detectors, with more than 72,000 boardings and 15,000 facility inspections conducted each year.

USCG uses the IMO sanctioned Automatic Identification System (AIS), which is the global standard for ship-to-ship, ship-to-shore, and shore-to-ship communications, as the basis for its Nationwide Automatic Identification System (NAIS). NAIS was initiated in response to the MTSA to enhance domain awareness with a focus on improved security, navigational safety, search and rescue, and environmental protection services.

All information collected by the USCG and CBP which is provided to NTC-C allows CBP and USCG to track where vessels, shipping containers, and crew have been and their locations prior to entering the U.S. In addition to tracking these cargo vessels, USCG and other law enforcement agencies face the challenge of distinguishing between legitimate small vessel operators and those involved in illicit activities. DHS's April 2008 Small Vessel Security Strategy (DHS 2008 Strategy) characterizes small vessels as any watercraft regardless of method of propulsion, less than 300 gross tons. Vessels less than 300 gross tons can include: commercial fishing vessels, recreational boats and yachts, towing vessels, uninspected passenger vessels, or any other commercial vessels involved in foreign or U.S. voyages. USCG statistics indicate there are approximately 17 million small vessels operating in U.S. waterways.

The goal of the DHS 2008 Strategy is to reduce potential security and safety risks from small vessels through adoption and implementation of a coherent system of regimes, awareness, and security operations by striking a balance between fundamental freedoms, adequate security, and continued economic stability. The DHS 2008 Strategy identified concerning scenarios which included a waterborne improvised explosive device. DHS and the USCG have strategies and programs in place to reduce small vessel risks, but the 2010 GAO report found there were still areas of concern including: loss of funding to support community outreach efforts; the lack of small vessel tracking systems; and funding constraints limiting security activities. The 2010 GAO report noted concerns stated in 2006 by then-Vice Admiral Thad Allen, Chief of Staff for the USCG, regarding concerns about small vessels posing a greater threat than containers for nuclear smuggling in testimony before the Senate Committee on Appropriations Subcommittee on Homeland Security.

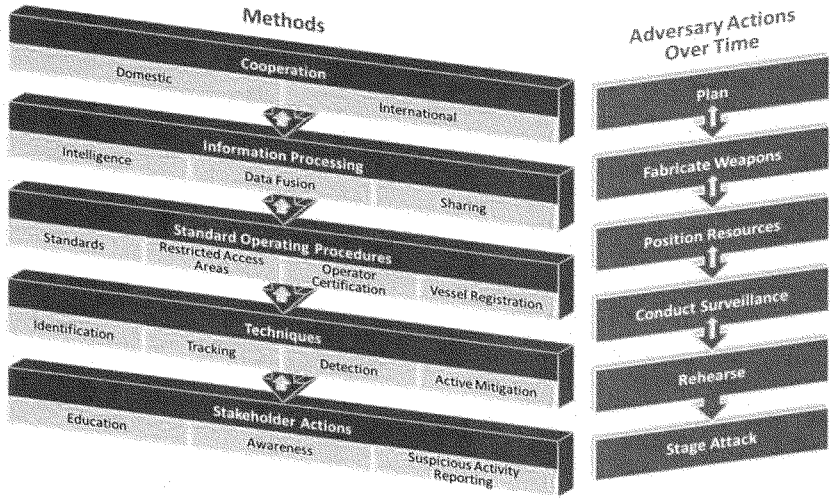
DNDO has tested boat-mounted radiation detectors, backpack carried detection equipment, and handheld radiological detection and identification devices. The January 2009 GAO report, "*Nuclear Detection – Domestic Nuclear Detection Office Should Improve Planning to Better Address Gaps and Vulnerabilities*", noted that DNDO tests revealed issues with the technology. Boat-mounted radiation equipment could not indicate the direction of the radioactive material causing the alarm. Backpack equipment works best when worn but it impeded USCG personnel when maneuvering on boats. Lastly, hand-held devices were expensive ($15,000 per unit) and did not float and did not withstand being submerged. The 2009 GAO report recommended DNDO take steps to work with the Departments of Defense, Energy, and State to develop an overarching strategic plan to guide efforts to combat nuclear smuggling. It also suggested that for DNDO's future efforts to combat nuclear smuggling on small vessels, DHS must develop criteria to assess the effectiveness, cost and feasibility of its pilot programs.

In 2011, DHS developed a Small Vessel Security Implementation Plan (Small Vessel Plan) after a multi-year process involving public and private stakeholders, DHS, and other federal, state, local and tribal authorities. The Small Vessel Plan is roadmap to realize the goals and objectives of the DHS 2008 Strategy. The Small Vessel Plan identifies possible and proven means of managing and controlling risks posed by the potential threat and possible dire consequences of small vessel exploitation by terrorists. The Small Vessel Plan been designated Security Sensitive Information due to its sensitive nature.

DHS released a report entitled *Small Vessel Security Implementation Plan Report to the Public* (Small Vessel Report). The Small Vessel Report notes the Small Vessel Plan employs a layered approach to achieve a defense in depth strategy against potential threats (see graphic on page 11).

DHS states that each layer of defense takes advantage of governmental authorities and capabilities, at times in coordination with stakeholder groups present, to disrupt adversary actions. While building on capabilities to act on information, the methods increase the potential of disrupting potential adversarial attacks and identify dangerous conditions and situations to allow for more effective responses to the broad array of situations that may be encountered in the maritime environment. These actions can improve readiness and responses to events and recovery from disasters. Federal partners, in conjunction with public and private stakeholders, build an informational system that facilitates and supports maritime homeland security.

DHS figure on the layered approach to achieve a defense in depth strategy:



WITNESSES

Panel I

Rear Admiral Peter J. Brown
Assistant Commandant for Response Policy
United States Coast Guard

Dr. Huban A. Gowadia
Director
Domestic Nuclear Detection Office

Mr. Todd C. Owen
Assistant Commissioner
Office of Field Operations
U.S. Customs and Border Protection

Mr. David C. Maurer
Director
Justice and Law Enforcement Issues
Homeland Security and Justice Team
U.S. Government Accountability Office

Panel II

Dr. Gregory H. Canavan
Senior Fellow
Los Alamos National Laboratories

Dr. Charles A. Potter
Distinguished Member of the Technical Staff
Sandia National Laboratories

Mr. Joseph M. Lawless
Chairman
Security Committee
American Association of Port Authorities

Dr. Stephen E. Flynn, Ph.D.
Director
Center for Resilience Studies
Northeastern University

PREVENTION OF AND RESPONSE TO THE ARRIVAL OF A DIRTY BOMB AT A U.S. PORT

TUESDAY, OCTOBER 27, 2015

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COAST GUARD AND MARITIME TRANSPORTATION,
COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE,
Washington, DC.

The subcommittee met, pursuant to call, at 10:01 a.m., in room 2167, Rayburn House Office Building, Hon. Duncan Hunter (Chairman of the subcommittee) presiding.

Mr. HUNTER. Good morning. The subcommittee will come to order.

Before I get into my statement, I want to indicate my displeasure at the lack of response from the Secretary of Homeland Security regarding a letter I sent on October 7th for this hearing asking for information related to today with what we are going to talk about.

I specifically asked about the number of containers inspected prior to arrival at a U.S. port, the percentage inspected after arrival, the different inspection methods used and criteria used to determine increased or reduced screening. So basically I asked them: How many containers do you screen? How do you screen them? How do you scan them? You would think that the Department of Homeland Security would have those numbers in front of them because that is what they do.

In addition, I asked about the Department's progress to meet the 100-percent container scanning requirement in the 9/11 Commission Act of 2007 for containers headed to U.S. ports. The information requested is relevant to today's hearing, and the Department should have been able to provide a response within a 3-week lead time, roughly the same amount of time taken to develop the testimony we will hear from Department witnesses today.

Are any of you aware of the status of the Secretary's response to my letter I guess would be the first question.

Mr. OWEN. Yes, sir. I am aware that the letter has cleared the interagency with the departments within, and it is waiting for final approval at the Department level.

Mr. HUNTER. Of the numbers?

Mr. OWEN. I am aware of the numbers, sir. Yes, sir.

Mr. HUNTER. So you have the numbers?

Mr. OWEN. I have the numbers prepared for today, sir. Yes, sir.

Mr. HUNTER. Great. OK.

And let me say one last thing, too. We are not going to hear from anybody from SOUTHCOM [U.S. Southern Command], and we are

not going to hear from anybody from NORTHCOM [U.S. Northern Command], because the OSD, the Office of the Secretary of Defense, refused to send witnesses or briefers from either SOUTHCOM or NORTHCOM.

I am not sure whether that was the Department of Defense saying this is a Department of Homeland Security issue and a Department of Homeland Security issue only or whether they just didn't care enough to send somebody. Maybe they have a beef with me. And I would say to OSD that that is pretty petulant, to not send anybody from any—besides the Coast Guard from the Department of Defense, from NORTHCOM or SOUTHCOM.

The subcommittee is meeting today to discuss the scenario of a dirty bomb—a radiological dispersal device—in a U.S. port; the potential for how such a device could be brought in; measures that can be taken to deter, detect, and interdict the security threat; and ways to prevent an adversary from reaching its intended target within the U.S.

The United States has an exclusive economic zone spanning 3.5 million square miles, 95,000 miles of open shoreline, over 360 ports, and numerous small harbors across the country. Our maritime border is unique compared to our land or air borders due to its sheer size and the potential ease of moving large quantities of materials undetected.

Interdiction efforts are about more than the seized contraband. Understanding the pathways used by smugglers is a critical part of the process. Pathways used for drugs today could be used to bring in anything—nuclear, radiological material, or anything. If you can carry thousands of pounds of something, you can carry thousands of pounds of something else. Knowledge of existing smuggling practices coupled with trends on how actions change due to law enforcement efforts can assist in disrupting future smuggling efforts.

After 9/11, security measures were enacted to better protect our homeland by expanding efforts to detect and deter threats overseas. It is obviously much better to find things if they are not on U.S. shorelines. These efforts include screening cargo manifests before containers are loaded onto a U.S.-bound ship, scanning shipping containers that have been determined to be high-risk, screening ship personnel data, knowing where a ship and its cargo have been before entering United States territory, and intercepting a vessel at sea and preventing its entry into a U.S. port.

We will hear from our witnesses today on how the Federal Government deploys a whole-of-government, layered approach, including law enforcement, technology, and intelligence, to detect, deter, and interdict potential threats.

These internal measures are combined with treaties and agreements with foreign governments to conduct cooperative enforcement efforts at ports overseas.

In early October, the Associated Press reported on the FBI [Federal Bureau of Investigation] and Eastern European authorities' efforts over the last 5 years to successfully interrupt four attempts by criminal gangs with suspected Russian ties to sell cesium to Middle Eastern extremists. And we can talk about cesium either in this panel or the next panel. It is not the most dangerous stuff, but

it is still bad stuff. The successful disruption of the sale was a positive result; however, the desire of our adversaries to obtain, at a minimum, materials for a dirty bomb or, to the extreme, materials for a nuclear weapon are growing.

Due to the Iranian deal, no matter what you think about it one way or the other, and the reaction that the other Middle Eastern countries are going to have to Iran having nuclear facilities, there is going to be more nuclear material out on the market. That is just the way it is going to be going forward. Over the next 10 or 25 years, you are going to have more countries with more nuclear capability than we have probably ever seen in the world.

And I think that is one of the reasons we are going to kind of start this series of hearings up, is because the interdiction efforts by the Coast Guard and Department of Homeland Security are going to be paramount. I mean, that is the only line of defense, not just the first line of defense, that we have in this country.

It is concerning that the administration's whole-of-government approach does not appear to include foreign nuclear policy. For an administration that proclaims to be anti-nuclear-proliferation, we are heading down a path where our adversaries will have greater access to nuclear material. While this hearing is about preventing, deterring, and interdicting threats from coming onto our ports, it is important to be aware of how our foreign policies may conflict and potentially disrupt enforcement measures to keep our country safe.

With that, I yield to Ranking Member Garamendi.

Mr. GARAMENDI. Mr. Chairman, thank you very much for the hearing.

When you first noticed the hearing, I am going, "Wait a minute, I have been here, I have done this. What is—when did it occur?" About 2005, we did a national meeting on natural disaster insurance. Including among the three things that we looked at in 2005 was, let's see: Hurricane up the east coast—that would be Sandy; earthquakes at the New Madrid fault, but that hasn't happened, thankfully; and terrorism, a dirty bomb at the Port of Long Beach. So there is a study out there. I really wanted to get it in time for this, but I wasn't able to gather it.

In any case, this is a subject that we need to pay attention to, and I thank you for holding the hearing.

The threat of a nuclear or radiological dirty bomb arriving at a U.S. port is sobering. It certainly was in 2005 when we did that national review of disaster insurance. An idea that was virtually unimaginable 15 years ago—well, not quite 10 years ago—is now the primary focus of coordination, multilayering strategy involving multiple Federal agencies, including the U.S. Coast Guard.

By most accounts, it would appear that the Global Nuclear Detection Architecture and numerous Federal programs, activities, capabilities that are implemented to fulfill this strategy seem to be meeting the challenge of keeping radiological or other nuclear threats outside of the U.S. homeland. This is something we ought to be grateful for, and I certainly appreciate that because of the effort made by thousands of Federal employees every day to protect us.

And yet we cannot let our guard down, for even the likelihood of a terrorist cell smuggling weapons of mass destruction into the country in a shipping container may be low but the consequences would be catastrophic. At least, that is what we learned in 2005. And because the risks are potentially catastrophic, we must continue to do everything possible to make sure it doesn't happen.

Among the questions we are going to be asking, or, at least, I will be asking—I assume you will also, Mr. Chairman and Members: Are we adequately testing and validating our technologies and procedures and training to make sure that they remain relevant given the current and emerging threats and circumstances?

Second, in the event of a detonation of a dirty bomb at a U.S. port, are we making sure today that we will have in place the technologies and capabilities to quickly and effectively respond to the cleanup and recovery of such an attack? I know on the insurance side the answer in 2005 was "no," and today I am sure it is also "no."

And, thirdly, considering that a future terrorist may be homegrown, are we doing everything we can to track and monitor within the U.S. the coastwide trade to make sure that vessels operating in U.S. domestic waters are not a potential conduit for those seeking to do us great harm?

It is going to be an interesting hearing. Thank you for the panels. I thank the witnesses who are here. And looking forward to the testimony.

Thank you.

Mr. HUNTER. I thank the ranking member.

I am going to introduce everybody really quick.

Rear Admiral Peter J. Brown, the U.S. Coast Guard's Assistant Commandant for Response Policy. Thanks for being here.

Dr. Gowadia—did I get it right?—the Department of Homeland Security's Director for the Domestic Nuclear Detection Office.

Mr. Todd Owen, the Department of Homeland Security's Assistant Commissioner for the Office of Field Operations for U.S. Customs and Border Protection. Thanks for being here.

And Mr. David Maurer, the U.S. GAO [Government Accountability Office] Director of Homeland Security and Justice.

And we will start with you, Admiral Brown. You are recognized.

TESTIMONY OF REAR ADMIRAL PETER J. BROWN, ASSISTANT COMMANDANT FOR RESPONSE POLICY, U.S. COAST GUARD; HUBAN A. GOWADIA, PH.D., DIRECTOR, DOMESTIC NUCLEAR DETECTION OFFICE, U.S. DEPARTMENT OF HOMELAND SECURITY; TODD C. OWEN, ASSISTANT COMMISSIONER, OFFICE OF FIELD OPERATIONS, U.S. CUSTOMS AND BORDER PROTECTION; AND DAVID C. MAURER, DIRECTOR, HOMELAND SECURITY AND JUSTICE, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Admiral BROWN. Well, thank you. And good morning, Chairman Hunter, Ranking Member Garamendi, and distinguished members of the subcommittee. I am honored to be here today to discuss the Coast Guard's role in the prevention and response to the arrival of a radiological dispersion device, or dirty bomb, into a U.S. port.

And I thank you for your strong support of the Coast Guard and our men and women in uniform.

It is a pleasure to be here today with two of our most important partners within the Department of Homeland Security: Customs and Border Protection and the Domestic Nuclear Detection Office. The Nation is safer in no small part due to the partnerships that we have with these two organizations. And I would like to personally thank both Dr. Gowadia and Assistant Commissioner Owen for their ongoing support and leadership.

My complete statement has been provided to the subcommittee, and I ask that it be entered into the record.

Mr. Chairman, through a layered security approach, the Coast Guard pushes border and port security out well beyond our Nation's shoreline and the exclusive economic zone by fostering strategic relationships with partner nations to detect, deter, and counter threats as early and as far from U.S. shore as possible in order to prevent an attack on the homeland.

The Coast Guard's efforts to prevent dirty bombs from nearing the U.S. ports and shores begins overseas with robust international partnerships that provide access to maritime ports of origin. Through our International Port Security Program, the Coast Guard performs overseas port assessments to confirm that foreign trading partners meet international standards for security and antiterrorism. Since the inception of this program in 2004, Coast Guard personnel have visited more than 150 countries and approximately 1,200 port facilities.

To more effectively counter these threats in the offshore region and throughout this hemisphere, the Coast Guard maintains more than 40 maritime bilateral law enforcement agreements and 11 bilateral Proliferation Security Initiative, or PSI, ship-boarding agreements, which allow Coast Guard teams to board vessels suspected of carrying illicit shipments of weapons of mass destruction, their delivery systems, or related materials far from shore.

The Coast Guard's membership within the intelligence community provides global situational awareness, analysis, and interagency collaboration with various components, including the CIA [Central Intelligence Agency], National Counterterrorism Center, and the FBI, among others. Through our Maritime Transportation Security Act, we provide security plan compliance and inspections for maritime facilities and vessels, and this reduces the vulnerability to terrorist attacks in or involving our ports.

Building on these preventive efforts, the Coast Guard also brings agility and mobility to our detection regime with the ability to deliver our detection capabilities anywhere in the maritime domain. The Coast Guard conducts over 400 routine vessel inspections, examinations, and law enforcement boardings every day. And Coast Guard personnel who visit boats, vessels, and regulated facilities carry detection devices to alert the users to the presence of radiation.

In 2004, we developed a Maritime Radiation Detection Program and have since maintained a close relationship with DNDO [Domestic Nuclear Detection Office] to standardize our equipment and enhance our national capacity for detection with multiple levels of capability, including the ability to reach back to scientific experts

for more information. We do this in conjunction with CBP [U.S. Customs and Border Protection] and with TSA's [Transportation Security Administration's] Visible Intermodal Prevention and Response, or VIPR, Program.

Many of our units, including our Coast-wide sectors, our deployable specialized forces, and our major cutters, are equipped with these devices that can identify specific isotopes, distinguish between man-made and natural sources, and, as I said, reach back to interagency experts for assistance.

Specifically, our Maritime Security Response Team, or MSRT, provides the Nation with a unique maritime capability for nuclear and radiological detection, identification, and self-decontamination in routine or hostile situations. The MSRT is specifically designed and exercised to integrate with other interagency or DOD [Department of Defense] response forces.

At the national level, together with CBP's National Targeting Center, the Coast Guard screens ships' crew and passenger information for all vessels that are required to submit what we call an ANOA, advance notice of arrival, 96 hours or more prior to entering port. In 2014, that process screened over 124,000 notices of arrival and over 32 million crew and passenger records.

The Coast Guard's response to a dirty-bomb threat would be part of a coordinated interagency effort to bring the most capable and appropriate resources to bear. If a dirty bomb is suspected en route to or identified within a U.S. port, the interagency Maritime Operational Threat Response protocol, or MOTR, would be employed to coordinate whole-of-government interagency action to achieve the best solution.

And, with that, sir, thank you.

Mr. HUNTER. Thanks, Admiral Brown.

Doctor?

Ms. GOWADIA. Good morning, Chairman Hunter, Ranking Member DeFazio, and Ranking Member Garamendi, and distinguished members of the subcommittee. Thank you for the invitation to testify with my colleagues from the Department of Homeland Security and the Government Accountability Office on our efforts to prevent and respond to the introduction of a dirty bomb into a maritime port.

An attack with a radiological dispersal device—that is, a dirty bomb—at a U.S. port would have profound and prolonged impacts to our Nation and the world. At the Domestic Nuclear Detection Office, or DNDO, we have a singular focus: preventing nuclear terrorism. It cannot be accomplished by any one agency, and, in fact, it takes a whole-of-enterprise approach. And so DNDO was deliberately established as an interagency office and benefits from the support of detailees from across the Federal Government.

In both our nuclear detection and forensics missions, we work closely with our Federal, State, local, and international partners and those in the national laboratories, in industry, and in academia. My testimony today focuses on DNDO's work to strengthen the operational readiness of our maritime partners to detect illicit radioactive material.

DNDO is responsible for the domestic implementation of the Global Nuclear Detection Architecture. The GNDA is a framework

for detecting, analyzing, and reporting on nuclear and other radioactive materials that are out of regulatory control.

Now, the tendency can be to place great focus on technology alone. It is, however, more effective to carefully integrate intelligence, law enforcement, and technical capabilities to improve the GNDA.

Indeed, our GAO colleague, Director Maurer, captured it well in a previous hearing, stating, "Detection technology is an important part of the overall effort to keep a nuclear device out of the U.S., but it is not the only one. Consider this," he said. "If the U.S. ever has to rely on a radiation portal monitor to stop a smuggled nuclear device, a lot of other things have already gone wrong. It means law enforcement missed it, the intelligence community missed it, our allies missed it, risk-based screening missed it, treaty regimes did not work, and nonproliferation programs failed."

Keeping his words in mind, our strategy is to provide effective technologies to well-trained law enforcement and public safety professionals as they conduct intelligence-driven operations. By implementing a multilayered, multifaceted, defense-in-depth approach, it is our objective to make nuclear terrorism a prohibitively difficult undertaking for the adversary.

And so our efforts to secure the homeland begin overseas, relying largely on sovereign foreign partners to develop and enhance their own national detection programs. In this endeavor, DNDO works closely with the interagency and multilateral partners to develop and share guidance, best practices, and training. The collective efforts abroad help ensure illicit radioactive material or devices can be interdicted before they arrive at our shores.

The layered approach continues at our borders. DNDO procures radiation-detection systems for use by DHS [Department of Homeland Security] operational components at our ports of entry, along our land and maritime borders, and within the United States. Today, all Coast Guard boarding teams are equipped with detection devices. DNDO has also acquired detection systems for the Coast Guard and Customs and Border Protection to scan small vessels before they reach our shores. And at our seaports of entry, CBP scans nearly 100 percent of all incoming maritime containerized cargo for radiological and nuclear threats.

Building operational capacity across the Federal, State, and local enterprise is also critical. And so DNDO is presently working with 33 of the Coast Guard's Area Maritime Security Committees, sharing information and intelligence, assisting with alarm adjudication, and providing technical support to our operational partners as they build their detection programs.

In case of an attack of nuclear terrorism or the interdiction of a nuclear radiological threat, leadership will need rapid, accurate attribution based on sound scientific evidence. Nuclear forensics, when coupled with intelligence and law enforcement information, supports those determinations. DNDO, therefore, advances technologies to perform forensic analyses on predetonation nuclear and other radioactive materials.

Make no mistake: The United States remains committed to holding fully accountable any State, terrorist group, or other nonstate actor that supports or enables terrorist efforts to obtain or use

weapons of mass destruction. At DNDO, we will continue to work with our partners to counter nuclear terrorism and improve our overall collaboration across the technical, intelligence, and law enforcement communities.

We sincerely appreciate the committee's support of our efforts to secure our homeland. Thank you for the opportunity to be here today. I look forward to your questions.

Mr. HUNTER. Thank you, Doctor.

Our next witness is Mr. Todd Owen, the Department of Homeland Security's Assistant Commissioner for the Office of Field Operations for U.S. Customs and Border Protection.

Mr. Owen, you are recognized.

Mr. OWEN. Good morning. Chairman Hunter, Ranking Member Garamendi, esteemed members of the subcommittee, thank you for the opportunity to testify today on the role of U.S. Customs and Border Protection in preventing and responding to the threat of a radiological weapon at our ports of entry, an important responsibility we share with our partners here today.

As the lead DHS agency for border security, CBP works closely with our domestic and international partners to protect the Nation from a variety of dynamic threats, including those posed by containerized cargo arriving at our air, land, and seaports.

Before my appointment as the Assistant Commissioner of CBP's Office of Field Operations earlier this year, I served as the Director of Field Operations for the Los Angeles-Long Beach Seaport, and I have also served time as the Executive Director responsible for all of CBP's cargo security programs. I know firsthand how complex cargo security operations are and how valuable our programs and partnerships are to our national security.

Since the September 11 terrorist attacks, CBP has established security partnerships, enhanced our targeting and risk assessment programs, and invested in advanced technology—all essential elements of our multilayered approach to protecting the Nation from the arrival of dangerous materials, such as a dirty bomb, at our ports of entry.

CBP has several key programs that enhance our ability to assess cargo for risk, examine high-risk shipments at the earliest possible point, and increase the security of the supply chain. I would like to highlight just a few of these efforts for you today.

Since 2002, CBP has been receiving advance information on every cargo shipment, every vessel, every crewman before they arrive at our ports of entry. For maritime containerized cargo, this information is received 24 hours prior to lading the cargo in the foreign seaport.

This advance information is then run through CBP's Automated Targeting System, which will compare the data against multiple law enforcement and trade databases. Those shipments identified as high-risk will be selected for examination.

High-risk shipments may be examined overseas before being laden onto the vessel heading for the United States as part of CBP's Container Security Initiative. CBP's CSI program places U.S. officers in 60 foreign seaports in 35 countries around the world. These overseas CBP officers have the ability to reach 80 percent of the maritime cargo heading to the United States. All over-

seas examinations are performed with the assistance of our host-country counterparts.

Every cargo inspection conducted overseas includes a scanning of the container for radiation, as well as subjecting the shipment to a nonintrusive inspection. A nonintrusive inspection uses systems of high-energy x ray or gamma ray to look into the container for anomalies which may be of concern. In fiscal year 2015, CBP performed over 124,000 overseas examinations of high-risk cargo before the cargo was placed on a vessel destined to the United States.

If the exam is not performed overseas at a CSI seaport, the shipment will be inspected upon arrival at a U.S. port of entry. At the U.S. ports of entry, CBP also deploys the same large-scale, nonintrusive inspection systems to quickly examine containerized cargo for the presence of anomalies which may indicate a threat. Those containers found with anomalies in their cargo are physically searched at warehouses located in the seaports.

Lastly, every containerized shipment leaving a U.S. seaport, every single shipment, is scanned for radiation and has been since 2010. There are over 1,280 radiation-detection portal monitors deployed at our U.S. border crossings, allowing for nearly 100 percent radiation screening of——

Mr. HUNTER. Mr. Owen, you just said that 100 percent of cargo leaving U.S. ports?

Mr. OWEN. Leaving U.S. ports, yes, sir.

Mr. HUNTER. "Leaving" is correct?

Mr. OWEN. Yes, sir, 100 percent.

So the 1,280 radiation portal monitors allow us to scan nearly 100 percent of the arriving seat containers, trucks, and passenger vehicles arriving from Canada and Mexico, as well shipments in the mail and aircargo environments. So most Americans are unaware of this critically important security measure in place at U.S. ports of entry throughout the country.

CBP's detection technology, targeting capabilities, and partnerships are strategically aligned to prevent the arrival of a dangerous weapon like a dirty bomb at a U.S. port. However, if such an event were to occur, CBP has established contingency plans and standard processes to ensure a coordinated and effective response. In the event CBP detects or suspects radiological material, all personnel are trained in "secure, isolate, and notify" protocols. The suspect cargo is secured, the immediate area is isolated, and scientific experts are notified. CBP scientists at the CBP Teleforensic Center in northern Virginia will confer with the Department of Energy and, when necessary, refer the findings to the FBI to coordinate an appropriate response.

Thank you for the opportunity to testify today, and I am here to answer your questions.

Mr. HUNTER. Thank you very much.

And our last witness is Mr. David Maurer, again, the U.S. GAO's Director of Homeland Security and Justice.

Mr. Maurer, you are recognized.

Mr. MAURER. Good morning, Chairman Hunter, Ranking Member DeFazio, Ranking Member Garamendi, and other Members and staff. I am pleased to be here today to discuss DHS's efforts to prevent a dirty-bomb attack on a U.S. port.

Preventing the smuggling of a nuclear or radiological device into the U.S. is understandably and deservedly a top national priority. And, as we have heard from the other witnesses, there are a wide array of programs and activities at several Federal agencies to help address and mitigate this threat. Mr. Chairman, my statement today focuses on one key aspect of this much larger effort: DHS's covert operations to assess its capabilities to detect and interdict the smuggling of nuclear materials into the U.S.

Over the years, DHS has invested billions to develop, purchase, and deploy radiation-detection equipment on our Nation's borders, as well as equip and train DHS personnel on how to use this technology. DHS has invested substantially less on testing to see whether it is being properly used. For example, over a recent 5-year period, CBP spent $1 million for covert testing—and that is "million" with an "m"—and that spending covered all types of covert testing, not just nuclear and radiological.

Now, it is very important to give CBP credit. Through much of that period and up to the present day, they were only required to do a single covert test per year. CBP took it upon themselves to do more than that, roughly one or two dozen a year. While CBP did more than required, this resource investment meant that they could not test every port of entry.

In its covert tests, undercover CBP officers tried to smuggle radiological materials through U.S. ports of entry. Basically, this is a real-world test of the equipment and the personnel using it. We found that CBP's testing provided limited assessment of its rad/nuc-detection capabilities. Specifically, the number of covert tests was not sufficient to make a generalizable assessment of all U.S. ports of entry. Over an 8-year period, CBP conducted covert tests at 86 of the 655 locations where testing could have been done.

In addition, CBP's decisions on which locations to test were not based on risk assessments. That meant its covert testing did not prioritize the most dangerous materials, most vulnerable locations, and most critical equipment. For example, 31 percent of CBP's tests were done at fixed checkpoints within the U.S., not at ports of entry. We recommended that CBP use a risk-informed approach to help determine where to conduct its covert tests. CBP agreed and is in the process of doing just that.

We also reviewed what CBP did with the results of its covert tests. Over a 5-year period, these tests found problems with officer noncompliance with policy, equipment failures, as well as officer error due to lack of training. The good news is that CBP followed up on systemic problems like these to ensure corrective actions were taken. However, they did not consistently track the status of actions to fix problems at individual locations. We recommended that they do so, and they have actions underway to do that.

Mr. Chairman, in some respects, our findings on this program mirror some of the themes we have seen over the past several years. In general, the U.S. has made significant progress combating nuclear smuggling and enhancing the security of U.S. ports. In particular, we have made great strides since 1998, when the U.S. began deploying radiation-detection equipment.

At the same time, many of these programs could and should have been implemented better. Agencies sometimes failed to assess

whether their programs were working as intended or did not fully integrate risk assessments into their planning. In some cases, agencies rushed to failure to deploy technologies before they were ready. Over the years, DHS and other agencies have implemented GAO recommendations to address these problems and, as a result, strengthened their programs.

Looking ahead, Congress, DHS, and other agencies face some tough decisions. The multilayered Federal effort is complex, vital to our security, and certainly not inexpensive. As DHS and other agencies adapt to changing threats, upgrade or replace aging equipment, and enhance their capabilities, GAO will be there to provide Congress independent oversight of this critically important mission.

Mr. Chairman, thank you for the opportunity to testify this morning. I look forward to your questions.

Mr. HUNTER. Thank you, Mr. Maurer.

I am going to now recognize Members for questions, beginning with myself.

So let's just stay on this. You are satisfied that CBP took into account what you guys found and that they are making corrective action?

Mr. MAURER. Yes. They took the findings from our report from last year very seriously. They put together a team of folks within CBP to address those recommendations, and they have actions underway to fully address them. They are not all the way there yet. We are working with them on that. But they have taken actions.

Mr. HUNTER. Good. Thank you.

Mr. Owen, let's start with the questions from my letter with the numbers. And what is the percentage of shipping containers inspected prior to arrival at a U.S. port?

Mr. OWEN. Yes, sir. Every container, again, is assessed for risk. The highest risk inspections occur overseas. In fiscal year 2015, 124,000 of those containers were inspected overseas. That is about 1 percent——

Mr. HUNTER. So what is that percentage?

Mr. OWEN [continuing]. A little over 1 percent of the 12 million containers that arrive from foreign ports every year.

Mr. HUNTER. OK. But everything is analyzed——

Mr. OWEN. Everything is analyzed. Every shipment is——

Mr. HUNTER [continuing]. And screened, I guess you could say.

Mr. OWEN. Depending on how you define "screening" and "scanning." And there is confusion as to how those terms are used.

We do look at the advance data we receive from the shipper, in terms of the manifest, as well as from the importer, in terms of our importer security filing. We compare all of that data to what we have in our databases in terms of our Automated Targeting System, the intelligence information that is provided. And, from those reviews, certain containers will rise to the top, causing us greater concern. Those highest risk containers are the ones we look at overseas.

Mr. HUNTER. So what happens when you look at a country like UAE [United Arab Emirates] that have—they scan everything.

Mr. OWEN. Yes.

Mr. HUNTER. They have those passive systems set up—by the way, those are made in San Diego.

Mr. OWEN. Right.

Mr. HUNTER. But, anyway, they have those passive systems set up, and they scan everything, right?

Mr. OWEN. Yes, that is correct. Many countries have now deployed radiation-scanning equipment similar to what we have in the United States, you know, in seaports around the world.

The radiation scanning is very doable from a technology standpoint. The challenge becomes the x-ray imaging of the containers. Whether it is a high-energy, medium-energy, or low-energy system, it still takes human intervention to analyze the result of that scan.

So you have a radiation portal monitor that is a very effective passive system, will tell you if there is a source emanating from the container that is of concern. You then need to take a second step to have the x-ray technology see what is inside.

That is really the part of the process that slows things down. Most countries in the world use a risk approach like we do and only inspect those highest containers of concern through x-ray systems.

Mr. HUNTER. OK.

What percentage are inspected after they get here? So if 1 percent total——

Mr. OWEN. A little over 1 percent overseas, yes, sir.

Mr. HUNTER. And then what percentage when it hits U.S. ports?

Mr. OWEN. Here in the maritime environment, it is about 2.7 percent on top of the 1 percent. So we are looking at a 3.7-percent overall in the maritime arena.

Mr. HUNTER. The next 2.6 or 2.7 percent is the next level down——

Mr. OWEN. Yes, sir.

Mr. HUNTER [continuing]. From the highest risk stuff?

Mr. OWEN. Yes. And then the next level down is what we will inspect here in the U.S. seaports.

And, again, that is in the maritime environment. The rates are approximately 26 percent on the land border with Mexico. So we look at, obviously, a higher percentage of what is coming in from Mexico because of the narcotics threat.

Mr. HUNTER. And when you use the risk-based assessment on where you should do this at, are there any ports in particular? I mean, like Mr. Maurer said, when you were doing your own testing, you did not use your own risk-based approach on where you were going to do that testing at, right?

Mr. OWEN. Right.

Two aspects of this. Number one is high-risk containers will be examined at whatever seaport they come into. A lot of that is dependent on the shipping patterns of what is arriving from what parts of the world, you know, into what parts of the country. So you will see those.

The GAO's findings were specific to the testing that we do of ourselves and should we focus more on those ports that have a greater likelihood of finding that type of device as opposed to a more universal approach.

So their findings, we felt, were very fair, and we have taken those into building a new risk matrix that will allow the operational testing at the ports that have the more likelihood of finding

those types of containers. However, we will inspect high-risk containers wherever they enter the United States.

Mr. HUNTER. So let me just get this—because in 2007—was it 2007 was when you all passed the—I wasn't in Congress in 2007—that said—2006—100 percent of cargo will be inspected, right?

Mr. OWEN. Yes. That is correct.

Mr. HUNTER. So what happened was everybody said, "That is impossible. There is no way to do that."

Mr. OWEN. Well, what happened was, from 2007 through 2010, we ran a series of six pilots around the world: in Qasim, Pakistan; Southampton, the U.K.; Salalah, Oman; Puerto Cortes, Honduras; a terminal in Busan, Korea; and a terminal in Hong Kong.

From those 4-year pilots, we were able to identify and clearly document all sorts of challenges, from the technology, the logistical impact, the effect on the efficiencies of the throughput of the cargo, things down to weather that would impact the dependability of the machines. So, through our 4-year pilots, we were able to identify and catalog all of the challenges that we have found.

From that time, we didn't really move forward in pursuing that any further. Now, since then, the Department has reengaged on this issue and has committed to take a look at what can now be done, being 5 years from when these pilots last ended, in terms of the technology that is available, the relationship with host countries, an understanding of what technology, as you mentioned, in the UAE is now present at other locations.

And, again, throughout all of these pilots what we have learned is it is not the radiation screening piece that is troublesome; it is the x raying of these containers. And, again, the 100-percent scanning law requires both aspects, 100 percent scanning, 100 percent screening for radiation, and 100 percent x ray of all of the containers. And that becomes the troublesome piece.

Mr. HUNTER. And just for everybody's benefit who is here, the next panel are a bunch of smart people from labs who can tell us what can be seen and what can't be seen, as far as they can go in a nonsecret hearing.

That answers enough for now, Mr. Owen. Thank you.

One last question for Admiral Brown. If something did happen—and this is, I guess, just a general homeland security type of question—but if something did happen, can the Coast Guard talk to everybody? I mean, can you communicate with the CBP and can you communicate with the sheriff and the ports and everybody all at the same time right now?

Admiral BROWN. Yes, sir. There are systems in place called Area Maritime Security Committees that bring together port stakeholders, governmental and nongovernmental, to plan for, prepare for, and, in the case of an actual event, respond and set up an incident command system network that responds to an incident, whether it is a dirty bomb or some other type of incident in a port.

So at the tactical level, there are ongoing communications among all the port stakeholders. From unit to unit, vessel to vessel, patrol car to patrol car, there is no single communication system that integrates all of Federal, State, and local government, but——

Mr. HUNTER. So you are saying that there is not a communication system that integrates everybody?

Admiral BROWN. There is not a tactical radio system that communicates across all those entities—State, Federal, local, and industry. But there are coordination protocols and the incident command system that allows each agency to communicate with others and then to communicate to their own unit.

Mr. HUNTER. So satphone to satphone?

Admiral BROWN. So we use interagency operations centers, some of which are virtual, some of which are actual bricks-and-mortar facilities, to coordinate those operations.

And, again, in a significant incident, those entities would be brought together in an incident command structure so that the operational priorities for action would be taken, divvied up among the agencies. The agencies would go out and perform those, given the tasking to their individual tactical units.

Mr. HUNTER. OK. Thanks, Admiral.

Thank you all.

And, with that, I yield to the ranking member, Mr. Garamendi.

Mr. GARAMENDI. Thank you very much, Mr. Chairman.

I want to go into the budget and the availability of money. It looks like you have spent $2.4 billion on this overall project since 2013. Is that correct, Ms. Gowadia?

Ms. GOWADIA. I do not have the exact numbers at my fingertips, but across the enterprise that sounds about right for the Global Nuclear Detection Architecture.

Mr. GARAMENDI. I will take that back. It is since 1995 to 2013, $2.4 billion putting in place the technology.

And the question for the three of you is: Is this a money issue—that is, not enough resources, not enough money to get the job done?

Let's start with Admiral Brown.

Admiral BROWN. Sir, I would say that one of our challenges remains coordination. We have a great thing going now with DNDO, CBP, TSA. And, within our department, as we have implemented the unity-of-effort goals of the Secretary, one of the areas in which we are applying greater effort is to coordinate the acquisition, the technology, so that the physical devices that we are using and the doctrine and the tactics by which we use them are similar and coordinated across multiple agencies. And DNDO has the lead in that.

Mr. GARAMENDI. So in your annual budget request to Congress, do you need more money or less money for this specific purpose?

Admiral BROWN. Sir, for this specific purpose, we run our requirements through the Department and through DNDO.

Mr. GARAMENDI. OK.

Ms. GOWADIA. Good morning, and thank you for that question, sir.

We at the Domestic Nuclear Detection Office are the strategic sourcing partners for this particular mission in the Department. What that means is we have the responsibility to bring in all the requirements from all the operational components, work with the Department's Joint Requirements Council, and allocate the right resources to meet the mission need.

Very recently, we did something for the first time in the Department. We pulled together requirements from across the agency and

made a single purchase, not just for the equipment itself, one particular unit, thereby standardizing the capability across the operational components, but also the maintenance contract. In the long run, this will save the Department a good bit of money. So that has helped, certainly.

I would put in a slight plug for your efforts to pass our budget. The continuing resolution, sir, would put a significant clamp on our ability to support CBP, in particular, to replace some of the aging radiation portal monitors and support operations at high-volume ports.

Mr. GARAMENDI. Ah, yes. Back to sequestration and continuing resolutions.

Mr. Owen?

Mr. OWEN. Sir, and similar to the Coast Guard, we define our operational needs to the DNDO, who then will survey the technology that is available and procure those equipment on our behalf. So their funding purchases the equipment that we need in terms of rad/nuc detection.

Mr. GARAMENDI. OK.

Most of this has been dealing with dirty bombs. There is another whole aspect of this radiological material control that is over in the Department of Defense budget and the Department of Energy budget, having to do with the international transshipment and the effort to address that.

I will note that in the House version of the NDAA [National Defense Authorization Act] we cut that budget, which would seem to be unwise. I understand that the recently vetoed bill increased it at the Senate level—perhaps still insufficient.

I do note that we are spending some $30 million this year on an east coast missile defense system to protect us from an Iranian nuclear bomb. And that is a $3.5 billion investment, should it ever come to pass, and another $1.2 billion annual investment in missile defense systems.

So the question for the three of you is: Are we more likely to see a missile incoming or a bomb in a tugboat or a fishing boat or in a container?

Mr. Owen? A dirty bomb or otherwise bomb?

Mr. OWEN. I think the likelihood of a dirty bomb is mitigated by several factors. Beginning on the international arena, as you mentioned, the presence of radiological-detection equipment at ports of entry or border crossings throughout the world is much higher.

There is also the logistics aspect of international shipping. If you actually have your hands on a dirty bomb, you turn it over to a truck driver, who is going to take it to the port. The port will turn it over to the terminal operator, who will turn it over to a carrier. The carrier will put it on the vessel. That vessel may move to other ports, where it is offloaded. You lose control of your asset. So I think the nature of that works against supporting the dirty bomb in that container.

So there is much more detection than we have had in the past, and you would also, again, lose control of your asset for some time as it goes through the shipping channels. I think there are probably other scenarios where you retain control of that asset that may be more of a greater threat.

Mr. GARAMENDI. For example?

Mr. OWEN. General aviation, small boats.

Mr. GARAMENDI. Admiral? Small boats? General aviation?

Admiral BROWN. I would tend to agree with Mr. Owens' assessment, sir. I think the answer to your question probably would better come from the intelligence community, but I would say that, in addition to the dirty-bomb scenario in a container and the challenges associated with delivering one, that some of the other threats we would face would be from smaller boats. And whether they were radiological devices or other improvised explosive devices or small arms attacks, those are another area of port security that we take very seriously.

Mr. GARAMENDI. I think most of this hearing is going to be focused on other than that, but it would be useful for us to focus on that. I know we have had some previous testimony in other hearings about that piece of it.

My time has expired. I thank you very much, Mr. Chairman. I yield back.

Mr. HUNTER. I thank the ranking member.

Mr. Gibbs is recognized.

Mr. GIBBS. Thank you, Mr. Chairman.

Thank you for the witnesses and all the work you do to protect this country.

I guess, Mr. Owen, a year or so ago, some of us had the opportunity to visit the Shanghai port and Hong Kong port. And we saw at Shanghai, I guess, the radiation detectors, you know, the container semis coming through there. I think they were probably put in place in the early 2003 period after 9/11, correct?

What is the status for monitoring their effectiveness, their wear and tear, and the lifespan? And then to replace them, is there a plan? Or if there is new and better technology, is there a plan for replacement?

Mr. OWEN. To the ports in Shanghai or to——

Mr. GIBBS. Well, in general. I just saw that in Shanghai's, but——

Mr. OWEN. Right. We started deploying that equipment here with U.S. Customs and Border Protection in 2002. So it was right around that time that you would see this equipment deployed nationwide or around the world.

We anticipated about a 10- to 15-year life cycle at that time. This technology was new. We didn't quite know what to expect. It has held up very well. It has been the workhorse of radiation detection in our seaports.

They are now coming towards the end of that life cycle, so we do need to replace them. There is better technology, or the algorithms that support this technology have advanced from where we were in 2002.

The original equipment, again, just speaking for Los Angeles-Long Beach, the equipment that was deployed would receive about 300 to 400 radiation alarms a day of the roughly 13,000 containers that enter L.A.-Long Beach on a given day. Those were all nonthreat materials, naturally occurring radioactive materials, medical isotopes, those types of nonthreat. With the new algorithms that we now have within our radiation portal monitors, we have reduced

that number to about 35 to 50 alarms a day, so about an 86-percent reduction, by having science advance in the last decade and where the algorithms are in 2015 as opposed to where they were in 2002.

Mr. GIBBS. So there is a plan in place to, you know, replace those, you know, just like the private sector does, a business——

Mr. OWEN. There is, like, a refresh of all the algorithms behind the radiation portal monitors here in the States that have been taking place for the past year and a half. I would assume globally that same type of activity is underway.

Mr. GIBBS. I also wanted to ask you—I believe, if my memory serves me right, there is, like, a certified program of shippers, because, you know, stuff like—for example, coming out of China, there are a lot of containers coming out of China, obviously. And if you have shippers that you work with all the time, that are credible or go through certain procedures, you can certify——

Mr. OWEN. Right.

Mr. GIBBS [continuing]. Those containers?

Mr. OWEN. There is the Customs-Trade Partnership Against Terrorism program that we work with not only vessels but as well as importers, manufacturers, truckers. They adopt higher security protocols, and, as part of that adoption, we go out and we validate that they have implemented what they said they would. We will treat them as lower risk than an unknown company or——

Mr. GIBBS. So, in essence, you can segregate that somewhat——

Mr. OWEN. That is the intention of it, yes, sir, the higher risk from——

Mr. GIBBS [continuing]. So you can be more effective.

Mr. OWEN [continuing]. And the unknowns from the unknowns. Yes, sir.

Mr. GIBBS. I guess for the admiral: Once a specific pathway for smuggling is intercepted, how often is that used for interdiction? You know, when you find something, when you shut it down, does it open back up later on, the pathway?

Admiral BROWN. Transnational criminal organizations, sir, are very resilient. They react when we are successful, and so they will move the geography of their smuggling. They will sometimes change the conveyance and the timing in ways to try to thwart us. We combat that primarily with intelligence and intelligence-based operations so we can try to have our very limited offshore assets in the right places at the right time.

I would say, though, that I started my career as a boarding officer in the Caribbean in the mid-1980s. And, just this week, we interdicted fishing vessels and go-fasts that are trying to get from South America toward Puerto Rico and the U.S. Virgin Islands. So criminal organizations, in my opinion, never completely give up on something that works for them, and so we continue to monitor those same threat pathways even 30 years later.

Mr. GIBBS. It was just mentioned earlier, the real challenge is small aviation and small boats, you know, offshoring from somewhere else and getting through. I think, you know, that would be a real challenge. And I don't know how you handle that, but, you know, that has to be a real challenge.

Did you want to say something, Doctor?

Ms. GOWADIA. When it comes to small or general aviation, I would mention that all incoming general aviation aircraft are met by our CBP officers using radiation detectors. So we have even increased in the last 10 years our capability in the general aviation environment, thanks in large part to their efforts.

Mr. GIBBS. All right. Thank you.

Thank you, Mr. Chairman.

Mr. HUNTER. I thank the gentleman.

I guess, just dovetailing there, bad guys aren't going to send stuff on cargo ships; they are going to send stuff up the way that the bad guys are sending stuff up now, right? Which is small fast boats coming up from Central and South America. I mean, isn't that how they would get anything here? Semisubmersibles?

Meaning, do you think we are putting too much priority on the shipping container portion, when the bad guy is sending all the drugs up in small boats to go-fasts that are hard to interdict, of which we only get—what was SOUTHCOM's number? Thirty-something percent total of the 100 percent that we know of coming up from South and Central America, right?

Admiral BROWN. That is a fairly accurate statistic, sir. We do interdict somewhere in the 15 to 20 to 30 percent, depending on how you measure and what we believe the flow rate to be of those drugs that are bound ultimately toward the United States.

However, sir, those small vessels, semisubmersibles, almost never attempt to make landfall in the United States. The era of a go-fast vessel going from the Bahamas towards south Florida or a fishing vessel going from Colombia all the way to the Florida Keys are long over, sir. Most of the drugs that leave South America first make landfall somewhere in Central America and then take land pathways toward the border in much smaller packages, much more difficult to detect.

So the success that we have using offshore aircraft, highly capable offshore cutters, that really takes the multiton loads out of circulation. And because of the success we have had over the past decades, we see very few drug-smuggling vessels actually arriving in the United States. Small amounts of marijuana landing in California, some relatively small amounts of cocaine and marijuana landing in Puerto Rico.

So that particular pathway from South America toward the United States is not really a full maritime pathway. And so we don't see a significant threat of nuclear material along that pathway in the maritime. Certainly, it could be exploited. It would have to make landfall somewhere in Central America and then move on land pathways toward the U.S.

Mr. HUNTER. OK. I got you. Thank you.

And we are honored today to have the ranking member of the full committee, Mr. DeFazio, who is recognized.

Mr. DEFAZIO. Thanks, Mr. Chairman. Thanks for holding this. I served 8 years on the House Committee on Homeland Security, and a lot of these programs were very much a work in progress when I served there.

GAO, have you audited the C–TPAT [Customs-Trade Partnership Against Terrorism] program lately? I mean, when I served a num-

ber of years ago, we found significant problems in the integrity of that program.

Mr. MAURER. Yes, that is right. We looked at that program in roughly 2008. We have an ongoing review that just started just a month or two ago. So it is still underway, and we are very far from having our final findings, but we would be happy to come up and chat with you about what we are learning along the way.

Mr. DEFAZIO. OK. Thank you. Because that was a major vulnerability previously.

Now, Admiral, in terms of, you know, when you say that under the NOA [notice of arrival] you are going to have the registered owner of the vessel—real registered owner or a front?

When I was in Malta discussing these issues when I was on the Committee on Homeland Security, they were like, "No way we are going to give you the names of the people who own these ships because we will lose all of our business here." You know, that is what we provide. We provide cover.

Has that changed? Are we getting the names of the real owners?

Admiral BROWN. Sir, we typically get corporate names and holding companies.

Mr. DEFAZIO. Right, which are double-blind, triple-blind, lawyers' offices and—yes.

Admiral BROWN. Yes, sir. So what we scan against are the names of all of the ownership entities associated with the vessel, with the containers, and with the crewmembers and their hiring. So those are some of the areas that we look at to try to see beyond the individual names of the people on board or the company that is shipping a given container.

But we try to look at all of the corporate entities and their history behind the vessel itself, its cargo, the ports that it has been in, and the crewmembers and the hiring practices, as well, because we see some characteristics of companies that are engaged in the hiring of mariners that may be more problematic that an individual mariner, himself or herself.

Mr. DEFAZIO. OK. Thank you.

Dr. Gowadia, you mentioned the radiological monitoring of all GA [general aviation] aircraft coming in. What are we doing in a maritime environment for ships or boats or even large pleasure craft that cross international borders into the U.S.?

Ms. GOWADIA. So, as I mentioned in my opening statement, sir, all Coast Guard boarding teams carry radiation sensors. So all the boardings that the admiral mentioned certainly include the radiation-detection element.

We have also worked with our CBP and Coast Guard partners to give them some capability to detect the standoff ranges for small-vessel scanning. So whether they are scanning a marina for a 4th of July event or they have some basis or some reason to go up out at sea to look at a particular small vessel, they have now a capability not just that they can carry on their backs but in their boats as well.

Mr. DEFAZIO. OK.

Ms. GOWADIA. The Coast Guard also asked us to look at detecting from above. So we have a very interesting research project where we are looking at the ability to equip Coast Guard's fixed-

wing and rotary craft with detection systems so that they could scan out at sea from above, as well.

Mr. DEFAZIO. Excellent. Very good.

Admiral, on the AIS [Automatic Identification System], I mean, what about an exchange, a theoretical exchange, at sea? I mean, maybe the containers have been scanned, we know the risk, but a ship stops at sea and exchanges a container. I mean, theoretically, I guess if someone was watching every vehicle's AIS at every moment, you would know that, you know, perhaps these two ships came in very close proximity and there seemed to be no movement, but, I mean, we are not doing that.

Admiral BROWN. Right. And that type of rendezvous at sea, while it would be, I think, extraordinarily uncommon in a container ship environment, is a common thing we see in drug trafficking. And so we use a variety of systems, AIS being one of them, to try to detect if a vessel lingers somewhere for a longer period of time than expected or deviates from an economically viable route.

So, using AIS systems and other national sensors that are available, I think we would be able to detect if a laden container ship deviated from its track or significantly delayed en route in a non-economical way. And we would be able to then decide how to target that vessel either offshore or once it arrived in port for additional scrutiny.

Mr. DEFAZIO. OK. All right. Thank you.

Thank you, Mr. Chairman.

Mr. HUNTER. I thank the ranking member.

Mr. Sanford is recognized.

Mr. SANFORD. I thank the chairman.

A couple questions. One is, I notice that you had said that we monitor every container on the way out. Who cares? Why?

Mr. OWEN. We scan every container before it leaves the port of entry before it enters the commerce of the United States.

Mr. SANFORD. No, no. But you said in the reverse, on the way out of the country.

Mr. OWEN. No, on the way out of the seaport.

Mr. SANFORD. Out of the seaport.

Mr. OWEN. Out of the seaport.

Mr. SANFORD. On its way still in.

Mr. OWEN. No. The radiation portal monitors are positioned at the exit gates of the seaport before it gets on the roads and leaves the seaport environment.

Ms. GOWADIA. To enter the United States.

Mr. SANFORD. To enter the United States. So we are not monitoring on the way out. So I misunderstood that.

Mr. OWEN. You mean our exports?

Mr. SANFORD. Correct.

Mr. OWEN. No, we are not radiation screening exports.

Mr. SANFORD. Got it. OK.

Mr. OWEN. No, sir.

Mr. SANFORD. I guess in the post-9/11 environment, I wouldn't call it overreaction, it was, I mean, warranted reaction based on the tragedy that occurred on 9/11. But what we all know, whether from the civil liberties standpoint, from a variety of different standpoints, there was probably overreach in some cases because of oper-

ational things, were just flat out impossible to get to, and in other cases from a cost standpoint, they didn't prove that effective in deterring whatever it was that we were trying to deter in that particular sphere.

And I guess, as I listen to this, my question would be along the same lines. I mean, if you look at the briefing material, it says with a dirty bomb there is really not enough radiation to kill people. You look at the logistical component in terms of the improbability of use in that somebody trying to do it that way would, as you put it, lose control of their bomb. You look at alternatives to sort of masking where one would come from in terms of rendezvous at sea or other things. It becomes a relatively low-probability vehicle, but we are spending a couple billion dollars a year, as I understand it, in the gestalt on these different programs.

Is it overplay relative to the degree of risk that we are really confronting as a Nation in this particular sphere?

Ms. GOWADIA. Congressman, the way we calculate risk is we couple the likelihood with the consequences. And the consequence of a nuclear attack would be so catastrophic that we cannot afford to take our eye off this ball. We do need to remain vigilant, make sure that we have sufficient capabilities to detect and mitigate. This is the ultimate preventable catastrophe. We can't stop doing it.

Mr. SANFORD. But, again, let's back up just a second. I mean, we are looking at in essence a 1-percent real check rate on the way in, maybe you bump that up to maybe close to 4 percent. But the reality is that papers in Pakistan or papers in a lot of other places around the globe can be relatively mixed. That is ultimately what we are checking in about 95 percent of the cases, we are looking at that as to trigger a degree of further inspection or look. And that further inspection look is at less than a 5-percent rate.

So you would say the consequences are catastrophic, but we have already determined that we can't inspect every container, we are not doing so, and so we are inspecting less than 5 percent, and we are still spending a couple billion dollars a year.

Ms. GOWADIA. I apologize. I was thinking about the nuclear threat writ large.

Mr. SANFORD. Correct.

Ms. GOWADIA. We do need—I could not agree with you more—we need to level our investments across all the pathways, across all the layers, so that we are not overstrengthening any one element of our transportation system or the ways and means things can come into the Nation.

Mr. SANFORD. Well, I see I have only got 1 minute. Let me just come at you from a different angle. I guess what I am saying is this: If you look at break bulk, for instance in the Port of Charleston there is a lot of break bulk activity as well as containerized activity, the overwhelming majority of our inspection seems to be at the containerized level, not at the break bulk level. So if you wanted to bring something in bad, seems like you could do it break bulk.

Going back to what one of my colleagues was raising with regard to a small boat, the reality is if you leave Bimini in the Bahamas and you head for Fort Pierce, you are not inspected by an officer until after you have docked that boat. Well, at that point, you are

in the Intracoastal Waterway, you could have hopped off and let the boat go and it goes. I mean, in other words, the inspection is coming after the point of entry.

So if you really want to do harm, it just seems to me that there are a variety of other relatively porous vehicles by which to do so if you are looking at maritime traffic. So we are, again, spending a couple billion dollars a year on an overlay that gives us, I think, a false sense of security.

Ms. GOWADIA. Sir, again, really I could not agree with you more. We have to be careful to make sure that we apply our resources across the board, which is why we work with our interagency partners, our international partners, to begin with nuclear security, material security, build their own detection architecture so the law enforcement capabilities overseas are attuned and aware to when materials come out of regulatory control and can stop them before they are in any form of conveyance to the United States. And we will continue to work with our interagency partners to do that.

Mr. SANFORD. I thank the gentleman.

Mr. HUNTER. I thank the gentleman.

The distinguished gentleman from Maryland is recognized.

Mr. CUMMINGS. Thank you very much.

Mr. Maurer, your testimony describes GAO's review of the CBP's operational geo-testing division covert tests. Your review found several areas in which the CBP could do a better job of targeting its limited covert testing resources. Do you believe that the CBP has taken the steps necessary to identify systemic trends and systemic weaknesses and to resolve these trends and weaknesses in a timely manner when and where they are found?

And let me tell you why I am asking this question, this series of questions. I have found that so often, as in Katrina, we have a situation where we are talking to each other, telling us everything is going to be fine, and then we say when the rubber meets the road everything is going to be fine, but then when it comes time for the rubber to meet the road we discover there is no road.

So where are we? Talk to me.

Mr. MAURER. Sure. We had three recommendations to CBP in our report last year. CBP has taken actions to address all three of those recommendations. They have taken actions to try to use a more risk-based approach to target their limited resources for covert testing to areas that are of higher risk or on the technologies that were more costly to deploy and to use.

They have also done a better job of following up on the recommendations on the findings of their prior covert tests. So, in other words, when they found problems in the past, we want to make sure those problems have been recognized and those problems have been fixed. They have made improvements in that realm as well.

They haven't done enough quite yet for us to consider those recommendations closed, but they are very close, and we are pleased with the progress they have made. It has only been about a year since our report came out.

Mr. CUMMINGS. Now, is the deployment of DHS's screening and detection capabilities across our Nation's seaports done in a manner that corresponds specifically to the varying threat levels and

scenarios at each port or is the deployment simply based on a single standard that all ports are to meet, and if so, are all ports meeting the standard?

Mr. MAURER. The radiation detection equipment is deployed to ensure that every single container is scanned for radiation before it leaves the port and enters into the United States. So from that perspective, DHS is making investment decisions to ensure that everything is looked at before it is entered onto the roads in the United States.

Mr. CUMMINGS. Now, Admiral Brown, can you please discuss the steps being taken to counter the risk posed by the smuggling of people onboard vessels arriving at U.S. ports, and what trends are you observing in human smuggling onboard vessels?

Admiral BROWN. Thank you for that question, sir.

I will really address this in two different ways. We did have for quite a while a problem with stowaways on commercial vessels, but since the implementation of the International Ship and Port Facility Security Code and the reciprocal arrangement that I described in which we can go out and assess port security at international facilities, the number of stowaways on commercial vessels has dropped dramatically over the past decade. We are down in essentially single digits per month of stowaways on commercial vessels arriving in the United States.

Mr. CUMMINGS. As compared to what?

Admiral BROWN. As compared to what had been hundreds in the early 2000s. And the fiscal responsibility for the repatriation of those stowaways is on the shippers and shipping companies, and so the shippers and the ship captains are highly incentivized to prevent stowaways from coming onboard. So that problem has been mitigated substantially with a combination of international standards and appropriate financial incentives.

With regard to migrants coming on more traditional pathways from the Caribbean, South and Central America toward the United States, including Puerto Rico and the Virgin Islands, we do have a nationality and threat-screening process. In the case of Puerto Rico and the Virgin Islands, it involves biometric scanning of many of the people who are attempting to get in. And we have maritime repatriation agreements with Haiti, the Dominican Republic, the Bahamas, and Cuba that ensure that those migrants interdicted at sea are in very high percentages returned to their country of departure or origin.

Mr. CUMMINGS. Now, Mr. Owen, in your testimony you identified the Secure Freight Initiative and Pakistan as an example of the CBP's strong working relationship with our foreign partners. As I understand it, the Secure Freight Initiative was previously being implemented at several foreign ports other than the one in Pakistan. Is that correct?

Mr. OWEN. Yes, sir, that is correct. Secure Freight was our pilot program to test 100 percent scanning overseas, 2007 to 2010. Qasim, Pakistan, was one of the six locations we piloted in.

Mr. CUMMINGS. I see my time has expired, so I will have some questions in writing.

Mr. HUNTER. I thank the gentleman.

Ms. Hahn, my colleague from California, is recognized.

Ms. HAHN. Thank you, Chairman Hunter, Ranking Member Garamendi. Thanks for holding this hearing.

This has been of a huge concern for me really since 9/11. Actually when I came to Congress, I started the PORTS [Ports Opportunity, Renewal, Trade, and Security] Caucus because ports, I think, are so important to this country, they are the main economic engine. And yet I always had a sense that after 9/11 we spent a little more time, effort, and money on securing our airports than we did our ports. And when people ask me what keeps me up at night, it is a dirty bomb at the Port of Los Angeles or Long Beach.

You know, ships make 50,000 calls a year on our U.S. ports, they carry 2 billion tons of freight, 134 million passengers. They are incredibly important. And one dirty bomb at Long Beach-L.A., which accounts for about 44 percent of all the trade that comes into this country, would be disastrous.

We were able to finally quantify what those ports meant to our economy in 2002 when there was a labor dispute and the workers were actually locked out for 10 days. Everyone finally figured out that the closure of the west coast ports accounted for about $1 billion a day to our national economy.

So I am concerned. And I applauded Congress when they passed the 2006 SAFE [Security and Accountability for Every] Port Act and wanted 100 percent scanning of all cargo containers. And as we are hearing today, we are around 3 percent of scanning. Screening is very different than scanning. We keep moving that deadline. No one really seems to believe that we can ever do 100 percent scanning. And so that deadline just keeps being bumped down the road.

But it makes me extremely nervous. All the scenarios that you all are saying never could happen, like we had a panga boat that made land in Rancho Palos Verdes, about 1 mile from where I live, not too long ago. And do you all remember in 2002 and 2003 when ABC News smuggled depleted uranium through the Port of New York and the Port of Long Beach? No one detected it. It was, like, was in the size of a soda can, it was shielded by material that was bought off the shelf, and no one detected that in either port.

So I get that with resources we are doing this layered approach and risk-based approach, but I am still very concerned that we are not scanning. And by the way, there is a big gap between when they come into port and then scanning them before they leave on a truck. I am worried, and I thought this hearing was about what could happen at one of these large ports, a dirty bomb exploding, not to mention the lives. We have 5,000 men and women that work on the docks at Long Beach and Los Angeles every single day.

So I am still extremely concerned. And the next panel I am going to see if we can talk about technology that actually could scan 100 percent without slowing down commerce. But I am worried. And I think part of why our ports are vulnerable to this kind of terrorist attack is because of the disruption that it would cause to our national economy and the global economy, and also because I am not convinced all of our ports in this country have a good recovery plan if, in fact, something like this happened.

So I was going to ask Rear Admiral Brown, what are you doing to work with ports in their recovery plan? You know, if you imag-

ine the Port of Los Angeles or a couple of those ships overturned in the main channel, not to mention maybe thousands of lives that would be lost, folks not even being able to get there to work or to rebuild a ship or clear a main channel.

What are you doing that would convince us—and maybe the terrorists—that it wouldn't be such an attractive target, because we can get back up and running quickly? There was a question in there somewhere.

Admiral BROWN. Thank you for that question. I am going to have to go overtime to answer it, though, because it is fairly complex.

One of the things I would say is that through the Area Maritime Security Committee process, part of that is an exercise program that we call AMSTEP [Area Maritime Security Training and Exercise Program], and each port Area Maritime Security Committee can prioritize for itself what scenarios they think are the most important security-related scenarios.

Since about 2003, different ports around the country have done over a dozen—two dozen, actually—exercises that specifically address dirty bomb scenarios, and one of the elements of each exercise is recovery. We have learned through a variety of real-world events that the resilience of the maritime security system is vitally important to our population and to our economy.

And so we have developed a process called the Maritime Transportation System Recovery Unit, or MTSRU, that we have used in response to Superstorm Sandy. We used it actually in response to the Haiti earthquake, recognizing, that you do, that you don't feed the country or its economy through an airport, but in fact through the seaport.

So helping to recover that port from containers in the water, sunken vessels, damaged piers have all informed our processes so that we engage with industry, the Army Corps of Engineers, the Navy Supervisor of Salvage, and other Federal partners, as well as industry, to put recovery of the maritime transportation system on the fast track of priority for recovery in a scenario like this.

Ms. HAHN. And I know my time is up. I know Los Angeles has a port recovery plan. Are you convinced that every seaport in this country actually has at their disposal a recovery plan in the case of a major disaster?

Admiral BROWN. I couldn't tell you that every port has a plan as robust and partnerships as well exercised as the Port of L.A.-Long Beach, but it is a significant part of every Area Maritime Security Committee's responsibility.

Ms. HAHN. I would like to see that as being the Coast Guard's priority in working with ports.

Thank you, Mr. Chairman.

Mr. HUNTER. I thank the gentlelady.

The gentleman from Louisiana, Mr. Graves, is recognized.

Mr. GRAVES OF LOUISIANA. Thank you, Mr. Chairman.

Thank you for being here today. I just have a few quick questions.

Number one, Admiral, do you have any information on the percentages of vessels that are inspected that are actually coming into U.S. ports, and then any breakdown of foreign vessels as opposed to domestic vessels?

Admiral BROWN. Sir, I am afraid I don't have a specific percentage breakdown, because the inspection and examination regimes for U.S. vessels and foreign-flagged vessels are quite different. For foreign-flagged vessels, as a port state, we have relatively limited authority primarily related to safety and security of that vessel. And what we do are called "port state control examinations," and they are risk-based, based on the vessel's history, as I was discussing with one of the Members earlier, the ownership, the cargo shippers, and so on. And so some vessels are examined every time they come to a U.S. port based on their track record; for some, they may go years without being examined.

Mr. GRAVES OF LOUISIANA. Would you be able to just kind of gut—and obviously you could come back to the committee and provide information for the record—but would you know just off-the-cuff if we inspect more domestic or foreign vessels coming into U.S. ports?

Admiral BROWN. I would have to ask my staff to do some research and get back to you in writing.

Mr. GRAVES OF LOUISIANA. Would you mind, if you could provide that information on the——

Admiral BROWN. We would be happy to do that, sir.

Mr. GRAVES OF LOUISIANA. Thank you.

[The information follows:]

RESPONSE PART 1: In calendar years 2010 through 2014, an average of 9,220 distinct vessels made 78,068 port calls to the United States. The Coast Guard conducted a yearly average of 9,644 port state control (PSC) examinations and 8,718 international ship and port facility security (ISPS) examinations on these vessels during this period. The average yearly number of ships detained for environmental protection and safety related deficiencies during this period was 124. The average yearly number of ships detained for security related deficiencies during this period was 12.

Vessels are targeted by their Coast Guard inspection history; associations with owners, operators, charterers, flag states, and recognized organizations (often classification societies) with poor PSC performance history in the U.S., lack of recent Coast Guard inspections, vessel type and age, and last ports of call. More often than not, a vessel is targeted for examination due to its first arrival to the U.S. or because it has not visited the U.S. in more than 12 months. For the most part, ships are examined one or more times a year, except for ships recognized as quality ships by our QUALSHIP 21 program (these ships are subject to port state control safety examinations every 2 years and ISPS examinations every year, unless a threat is identified prior to arrival).

Additionally, the USCG imposes Conditions of Entry (COE) on any vessels arriving to the United States after calling on ports that the Coast Guard has determined to lack effective anti-terrorism measures, or from those ports that the Coast Guard cannot ascertain that effective anti-terrorism measures are in place. COEs are additional security measures that the vessel must implement while in identified countries. These countries and the list of COEs are found in the publicly available USCG Port Security Advisory (3–15), dated 22 June 2015. The USCG verifies COEs prior to, or immediately upon, the vessel's arrival to the United States. The USCG conducted 1,627 of these boarding in calendar year 2014.

RESPONSE PART 2: In calendar years 2010 through 2014, an average of 20,326 inspections were conducted on U.S.-flag inspected vessels. Currently, there are 11,867 active U.S.-flag inspected vessels. This equates to an average of 1.71 inspections per vessel.

Generally speaking, U.S.-flag inspected vessels are attended at least once a year. In addition, those in saltwater service are attended twice in any 5-year period for a drydock and internal structural exam while those in fresh-

water service are attended once in a 5-year period for a drydock and internal structural exam. Next, should a vessel be involved in a marine casualty, it is generally attended for a damage assessment and to witness/test any repairs. Finally, those vessels enrolled in the Alternative Compliance Program (ACP) or the Maritime Security Program (MSP) may be targeted for additional oversight inspections based on their compliance history, vessel age/type, owner operator history, outstanding deficiencies and/or classification society requirements and history of port state control detentions or domestically initiated operational controls.

Additionally, the USCG imposes Conditions of Entry (COE) on vessels arriving to the United States after calling on ports that the Coast Guard has determined to lack effective anti-terrorism measures, or from those ports that the Coast Guard cannot ascertain that effective anti-terrorism measures are in place. COEs are additional security measures that the vessel must implement while in identified countries. These countries and the list of COEs are found in the publicly available USCG Port Security Advisory (3–15), dated 22 June 2015. The USCG verifies COEs prior to, or immediately upon, the vessel's arrival to the United States. The USCG conducted 1,627 of these activities in calendar year 2014.

Admiral BROWN. With regard to U.S. vessels, because as the flag state we are responsible not only for the safety and security, but the safe manning, operation, and environmental standards on the vessel, they are subject to a different inspection regime that may subject them to more visits than a foreign-flagged vessel or less depending on the specific inspection regime.

Mr. GRAVES OF LOUISIANA. Thank you. A second question. I have seen, and am actually curious about the Department of Homeland Security's response as well, but I have seen statistics and somewhat dated that showed the percentage of vessels that are actually inspected, and I remember it being extraordinarily low and that raising serious concern. But can you talk about the some of the work that you are doing in the source and transit zones as well, which may suggest that the actual percentage of vessels inspected at U.S. ports may be deceiving? Does that make sense?

Admiral BROWN. It certainly does, sir.

Mr. GRAVES OF LOUISIANA. And then how that relates to transnational criminal organizations.

Admiral BROWN. Certainly. So with regard to both security with regard to a dirty bomb, the main subject of this hearing, but also with regard to protecting our borders from other transnational threats, our operation is based on layered security, where we attempt—and I have described earlier some of the partnerships that we have with regard to port security—to inspect port facilities for their security regime overseas.

With regard to specifically the source and transit zone for narcotics, we also have significant partnerships with countries in South and Central America that allow us to board their flagged vessels on the high seas, recognizing that many of these nations don't have robust coast guards or navies with the kind of offshore capability that we have. And so those partnerships allow us to detect and interdict drug shipments very far offshore, in the case of one interdiction I made at sea of a major cutter, over 1,000 miles west of the Galapagos Islands, with drugs that were destined for a maritime landing in Mexico, but then ultimately for the United States.

So we do, using our long-range aircraft, our long-range cutters, and detection and monitoring capabilities of the Department of De-

fense and other partners, we attempt to identify those targets as far away as possible, interdict them as far away as possible, but then whenever we can, prosecute in the United States so we not only take the drugs off the market, but we attack the criminal network behind those shipments.

Mr. GRAVES OF LOUISIANA. I am not sure if any of the Customs or DHS or any of you folks care to——

Mr. OWEN. In terms of your vessel inspection question, I would just like to note that every vessel arriving from foreign are boarded by U.S. Customs and Border Protection officers to take care of the immigration admissibility issue. So there is a Federal law enforcement presence on each one, not to the level of inspection for the issues that the Coast Guard looks for, but to determine the admissibility of those crew.

Mr. GRAVES OF LOUISIANA. Great. Thank you.

Commissioner, I would actually like to ask you one other question. You know, whenever I look across Government, you obviously have local law enforcement, you have State, and you have Federal law enforcement entities that are out there. In the State of Louisiana, particularly in the Baton Rouge area where I am from, the Pointe Coupee Parish sheriff—we have parishes instead of counties—has formed this organization known as JTF–7, Joint Task Force 7, that initially was seven of the surrounding parishes' sheriffs that were all grouped together and they were doing a lot of maritime security work.

What role do you see those folks playing, considering they are on the ground, they have better coverage in many cases than some of your folks do, but what role do you see them playing in port security, maritime security as part of the overall system?

Mr. OWEN. Yes, absolutely. I mean, our presence is limited in some of the ports, especially in some of the parishes. I was the port director in New Orleans for 4 years, so I understand the parish system. And the important role that the local county sheriffs will play in assisting us is that additional presence as to what is taking place. They will often come in contact with individuals that may be of concern as to what they are doing in those seaports. They will notify us. We'll respond out.

So very strong working relationships, particularly in small communities where all of the law enforcement community have to rely on each other because no single entity has the resources that they need. So clearly a strong role for that State, Federal, local partnership.

Mr. GRAVES OF LOUISIANA. Great. Thank you, Commissioner.

If the chairman will——

Mr. HUNTER. Sure.

Ms. GOWADIA. Well, I would just like to add that we certainly believe very strongly in our State and local partnerships, and we have been working with our Area Maritime Security Committees and also with our State and local partners in law enforcement, particularly in your backyard, to build capabilities across the State public safety and law enforcement agencies. In fact, today all 50 States, we have engaged with all 50 States beginning to build capabilities across our Nation.

Mr. GRAVES OF LOUISIANA. Great. Thank you very much.

I just want to make note that Sheriff Torres, who leads this thing, called me and told me a while back that apparently the Department of Homeland Security was no longer allowing the seven or eight sheriffs that are all part of this task force to apply for a Federal Homeland Security grant jointly, that they were required to separate out. I am not sure of the status of that, but I just wanted to put it on your radar.

Thank you.

Mr. HUNTER. I thank the gentleman.

Ms. Brownley, my colleague from California, is recognized.

Ms. BROWNLEY. Thank you, Mr. Chairman.

I think my first question is to Mr. Maurer. I represent a small port, but a deepwater port, on the coast of California, Port Hueneme, and a lot of automobiles come through that port. Big ships come in, and there are 6,000 automobiles coming off of those ships.

And so I was wondering if the GAO had reviewed the screening procedures for noncontainerized cargo versus containerized and if you had any specific recommendations for improving screening for noncontainerized cargo.

Mr. MAURER. Most of our work has been focused on containerized cargo, because that is where the bulk of the Federal investment has been. From a larger perspective, we have done work looking at the much broader interagency effort to make sure that terrorists and nation-states aren't getting their hands on radiological material or nuclear material that would allow them to construct a device and bring it into the United States through whatever mechanism.

So one of the themes of our body of work has been that the technology and the screening procedures are very important. But there are all these other programs that are designed to secure the material at the source or to work through treaty regimes or to ensure that we have a robust intelligence community or law enforcement presence that is sharing information among Federal, State, and local partners to identify plots well before someone is able to construct a device and bring it into a port.

Ms. BROWNLEY. And, Mr. Owen, can you talk a little bit about the screening process for noncontainerized?

Mr. OWEN. Yes, absolutely. For all of the bulk, the break bulk, the RoRo [roll-on, roll-off], as you see up in Port Hueneme there, dependent on how the cargo is discharged, it may still pass through a radiation portal monitor. If it does not, the officers will address that through handheld radiation isotope devices. So in the case of Port Hueneme, most of those roll-on, roll-off vehicles do pass through the radiation portal monitors. The bananas, the pineapples that are coming into Port Hueneme as well are often containerized in that warehouse there onsite and then actually comes through the radiation portal monitor.

So the radiation portal monitors are our primary detection methodology. However, we do have the handheld radiation isotope devices that we use on bulk, break bulk. And every CBP officer carries a personal radiation pager on their duty belt that will alert should they come in contact with any of that as well.

Ms. BROWNLEY. Well, thank you for that. Do you think small ports are more vulnerable than large ports?

Mr. OWEN. I think small ports are less vulnerable, because everyone seems to know everyone. And, again, in the case of Port Hueneme, you have those same vessels that call every 3 or 4 days, you have the same crewmen, you have the same stevedores, you have known entities working these. I think in that environment someone from the outside unknown who may be up to something no good clearly stands out.

We have strong relationships with the seaport communities. When the terminal operators, the longshoremen, the stevedores, when they notice something that is amiss, they reach out to either the Federal or the port police across the board.

Ms. BROWNLEY. Very good.

And, Rear Admiral, to follow up on Ms. Hahn's line of questioning, if there was a port that went down, are there contingency plans to keep trade moving?

Admiral BROWN. That is a great question. Thank you. Partly, since trade is not entirely a Federal responsibility, the private sector and their distribution shipping networks would adapt to any disruption, whether it was a natural or man-made disruption, in a port. Some of that could be directed or shaped by Federal response, including the actions of the Coast Guard captain of the port responsible for a port, who might need to shut down a port from certain activities for a time to allow, whether it was recovery or investigation, and would work with neighboring captains of the port to see if we could expedite the adaptation of shippers to the new conditions.

Ms. BROWNLEY. So each port is not necessarily aware of a specific contingency plan, it is just if something happens, you will adapt?

Admiral BROWN. Right. Each port has this Area Maritime Security Committee which has a planning process, but because the type and the duration of the disruption would be so dependent on the specific scenario, the vessels that happened to be in port on that particular day, it would be impossible to prescribe ahead of time a specific recovery plan for shipping in that particular port.

Ms. BROWNLEY. Thank you, Mr. Chairman. I yield back.

Mr. HUNTER. I thank the gentlelady.

We have a second panel now. We were just looking at their testimony, and it is in math, whatever language math is, it is in math.

But I just want to stress one last—we talked today about stuff coming in from known areas where you can do risk assessment. I guess my last question for all of you is, why wouldn't bad guys that want to get a bad device in the U.S. take the same routes as guys that want to get drugs into the U.S.? Meaning, why wouldn't you bring it up from Central or South America and work up through the land borders and sneak it across? Is that totally—is that crazy talk? Do you think that they would ship it in and have the manifest be honest and all that kind of stuff?

Ms. GOWADIA. So that is certainly one of the scenarios we consider in the Global Nuclear Detection Architecture when we analyze it. So we do look at multiple means and modes of bringing the vessel in. In fact, I would love to sit down and share with you a classified briefing where we analyze almost 400 elements of the ar-

chitecture and base it on defensive capabilities, offensive options, and then base our resources and our——

Mr. HUNTER. We will take you up on that. We are going to have a classified hearing on this exact thing, and we can talk there more.

Ms. GOWADIA. Excellent.

Mr. HUNTER. Ms. Hahn is recognized.

Ms. HAHN. Thank you, Mr. Chairman.

I guess I just want one more clarification from the three of you. I mean, we are basically banking on this layered approach, this point of origin when it leaves the port. Are the three of you sitting here today saying that you are 100 percent positive that a dirty bomb could not slip through and get to one of our ports under this security model?

Ms. GOWADIA. Ma'am, I don't think anybody could give you a 100-percent guarantee for that, but I can tell you that based on the incredible resources of our law enforcement officers, our intelligence community, and our technical community, we are bringing every last resource we have to bear. And if we didn't use all that was at our disposal in this layered, multifaceted approach, we would be more vulnerable. We are far better off today than we were 10 years ago.

Ms. HAHN. Would we be better off with 100 percent scanning?

Ms. GOWADIA. In a classified session, I would love to walk you through and explain to you why we probably would not be.

Ms. HAHN. Rear Admiral?

Admiral BROWN. Ma'am, the only thing I would add to that is that we have had over the past 12 years or so several scenarios in which there was a radiological or threat concern on a vessel coming in from overseas. And with the MOTR process begun, that is the Maritime Operational Threat Response interagency process, we are able to either board the vessel at sea and resolve the issue or bring the vessel to a safe place with minimal population to conduct an examination and resolve the issue.

And in one very specific case, not regarding a bomb threat, but a possible terrorist threat where it was ambiguous as to whether the vessel was going to a United States port or a Canadian port, we are able to do that same level of interagency coordination with our Canadian counterparts to very good effect.

So I am confident that the processes that we have in place are effective for recognizing and responding to these threats in a way that will mitigate the probable impact. But as Dr. Gowadia said, I couldn't say with 100 percent certainty that we can prevent a dirty bomb scenario.

Ms. HAHN. Todd?

Mr. OWEN. And I would also agree there is no 100 percent certainty. But with the 100-percent scanning, I think when you look strategically at where it does make sense, like what we are doing in Qasim, Pakistan, where every container coming out of Qasim is scanned, with what we started this year in Jordan, in Port of Aqaba, where every container coming out of Jordan is scanned, I think in those strategic locations that give us more concern, it is the right approach.

Ms. HAHN. Thank you.

Mr. HUNTER. I thank the gentlelady.

And we are not going to shake hands and stuff, because we have about a half an hour with the next panel. So thank you very much for your time and for what you do.

And we will have more hearings on this coming up, Ms. Gowadia, so we will have a classified, fun hearing.

Mr. GARAMENDI [presiding]. While the chairman is out, if the next panel would come up and take their places. Mr. Gregory Canavan, Charles Potter, Joe Lawless and Stephen Flynn. The chairman is out of the room for a few moments, but he asked me to begin your testimony. We do have a short period of time, so we will begin.

Mr. Canava, Canavan?

Mr. CANAVAN. Canavan, sir. It is Irish.

Mr. GARAMENDI. It is a fine name, then.

Mr. Canavan, please.

Mr. CANAVAN. Should I begin?

Mr. GARAMENDI. Yes, would you please.

TESTIMONY OF GREGORY H. CANAVAN, PH.D., SENIOR FELLOW, LOS ALAMOS NATIONAL LABORATORIES; CHARLES A. POTTER, PH.D., DISTINGUISHED MEMBER OF THE TECHNICAL STAFF, SANDIA NATIONAL LABORATORIES; JOSEPH M. LAWLESS, CHAIRMAN, SECURITY COMMITTEE, AMERICAN ASSOCIATION OF PORT AUTHORITIES; AND STEPHEN E. FLYNN, PH.D., DIRECTOR, CENTER FOR RESILIENCE STUDIES, NORTHEASTERN UNIVERSITY

Mr. CANAVAN. I am Greg Canavan. I am from Los Alamos. I submitted my testimony. Apparently the chairman doesn't want me to read the math, so I will summarize, if you don't mind, and ask that you submit it for the record.

I am very honored to be here. Thank you for inviting me. And I will not use math, I will just say a few words.

I am listed as a senior fellow from Los Alamos, that is my daytime job, but this is not necessarily a Los Alamos project. It is something that I have been working on, on and off, whenever I had a few minutes, ever since 9/11. On that day, the Department of Energy and the Department of Defense were kind enough to send an airplane out to New Mexico to get Dr. Hagengruber and I from—he is from Sandia—to come back here to pursue some projects that we had been looking into before 9/11 on unusual threats to the United States, one of which was a concern that there might have been nuclear materials here in the Capitol, perhaps in an operational form. And so we spent some time looking into that.

We were not looking for dirty bombs, we were looking for nuclear weapons, but the detection approaches are similar and also quite difficult. As Ms. Hahn pointed out earlier, groups have smuggled depleted uranium into the country fairly frequently. Actual enriched uranium is a little harder to find, but not that much easier. And so we were trying to find nuclear materials.

I might say that as an Air Force colonel and for the last 50 years or so, I have worked on designing nuclear weapons, testing nuclear weapons, occasionally flying nuclear weapons. But 9/11 was the first time I ever had to worry about the problem of trying to detect

nuclear materials, and I found it to be a very difficult and challenging business. There is not much signature from them at all. They are a lot harder to find in a way than dirty bombs. And we also found that although we have quite good techniques for defeating nuclear weapons—that is diffusing them once you have found them—that the business of trying to find them in the first place is very, very difficult.

After 9/11, I continued to work with the Department of Defense for a couple of years to try to remedy this problem. It was very frustrating, it was quite difficult, in part because I think we went off on the wrong direction. We recognized that neutrons, tiny particles of matter that don't carry any electrical charge at all, can go right through anything, through this building, through ships, through whatever, so they are a great way for candling nuclear materials. Particularly since when they hit a fissionable material they produce a lot more neutrons and enhance the signature, so that makes them a good thing to work with.

But we kind of got off on the wrong footing in that we adopted the idea that the right approach was to stand off 2, 3, 4 miles with an enormous particle accelerator from high-energy physics and try do the interrogation from there. It didn't improve your survivability if something went off, it just made everything a lot more complicated, and we kind of got discouraged with that approach.

But anyhow, we went that way. And so after a while, it just looked too hard, and we kind of gave up. And so the problem has not advanced very much from 9/11 to today in terms of detecting actual nuclear weapons.

So what has changed? And I think that there are five things that have changed. One is that a decade of development in nuclear sources and detectors have made much more practical schemes and automated schemes possible and even affordable, so that you could now have detector systems that could fit on ports, transporter vehicles, ships, whatever, and do, if you will, an inspection of all the things that came through the port for nuclear weapons.

What that leads to then, in the testimony that I handed in, it lends to a sort of modular deployment. That is, most stuff that moves today moves in TEUs, the 20-foot equivalent units that go on cargo ships now are now in the two TEUs, the 40-foot units that get racked up between the bulkheads in these big ships. And happily, if you use neutrons, particularly fast neutrons, they are very well suited to uniformly candling or inspecting such containers either in port or in transit. So I found that very interesting.

The second thing that hit me was a mistake that we made early on was to ignore countermeasures to the approaches that we were advancing for detection. We were sort of asked to go against a friendly adversary, if you will, somebody that made life easy for us. And that turned out to be not a favor, because we ignored the fact that there are absorbers, things like cadmium barium, that are used to control ordinary power nuclear reactors. They absorb neutrons very efficiently, so that one-thousandth of an inch of cadmium could knock the signals from a nuclear weapon down to almost nothing.

But then I realized that fast neutrons, neutrons up at the energy where they are born, could easily get around these absorptions and

produce big signals, and they were relatively insensitive to the known countermeasures.

There is the penalty that someone mentioned already. In radiography, when you are x raying something, most of your x rays go places that you are not interested in. For instance, in these big TEUs, if you are looking for a bomb that is maybe 10 centimeters across and the TEU is 3 meters across, only a fraction, maybe 1 percent of the neutrons actually hit the weapon to produce a signal and the rest of them act as noise. So that is a problem that you have to overcome.

But then the third thing, I realized after some thinking was that in the process of hitting the nuclear core, the neutrons sort of identify themselves. Instead of being at their initial energy, they kick out neutrons that have a spectrum all the way from 10 percent to 90 percent of that of the neutrons that are incident on them. They are easily identified, so they can be collected and you can throw away the noise very efficiently, particularly since the separation in energy of noise from the source is large and fairly specific and energy doesn't degrade much in the process of slowing down. Therefore you don't wind up with too many of the noise neutrons showing up in your bin where you are expecting your signal.

So those four things made life a lot easier, to the point where you can do very effective filtering on energy, which makes up and makes up more than for what you lose initially in the numbers of neutrons that missed the target. And so overall you can get signal-to-noise ratios at the appropriate energies, which are sort of halfway through the slowing-down process, signal-to-noise ratios of 100 to 1,000 or more, which means that you can have very confident detection of the nuclear materials with a very low false-alarm ratio of other materials.

Someone alluded to it in the previous talk, that the tough thing about x rays is that you never know what is going to be in one of these shipping containers. It may be axles, it may be electronics, it may be whatever. And even if you can radiograph one of these things 1 percent of the time, then you still have to go through some long screening process or unpacking process to figure out what the detected object actually was. With a very high signal-to-noise ratio nuclear signal, you have a fighting chance of passing everything through without having to go back and try to sort out what the problem was in the first place.

So it just seemed to have all of the characteristics that we were looking for. Even before 9/11, I was on the advisory committees for U.S. Space, Air Force Space, and North Command when it was first created, and we were sitting down trying to figure out how you should parcel out responsibility for detection.

Neutrons seemed to do everything that we had hoped that the Coast Guard would be able to do in its charter as the Service that would detect things before they got to the coast, eradicate losses and false alarms on the spot, and execute the first line of defense of the country.

Mr. HUNTER [presiding]. That is all right, Doctor. Thanks for being here. And we will come back to this stuff too.

Dr. Potter, you are recognized. And our next witness is Dr. Charles "Gus" Potter, Distinguished Member of the Technical Staff for Sandia National Laboratories.

You are recognized.

Mr. POTTER. Thank you. Chairman Hunter, Ranking Member Garamendi, and distinguished members of the Coast Guard, thank you for the opportunity to testify today on the topic of preventing and responding to an RDD [radiological dispersal device] attack. My name is Dr. Charles Potter. I am a systems analyst and a health physicist from Sandia National Laboratories in Albuquerque, New Mexico, and I have specialized in the RDD threat and radiological nuclear detection architecture for over the past 5 years.

The United States Government and many of our foreign partners have been working for more than a decade to reduce the risk of a successful radiological dispersal device attack. From an engineering standpoint, we define risk as a combination of the likelihood of the attack—that is, the degree at which an adversary has the intent, capability, and materials required—and the consequence of the attack. The RDD threat is a very complex and a multidimensional problem, and the U.S. Government has designed and implemented a variety of programs, based on scientific studies by Sandia National Laboratories and others, to reduce the likelihood of an RDD attack in terms of reducing the availability of material for exploitation, as well as identifying and impeding probable pathways from device to target.

However, the scientific understanding of the cost, time needed to clean up, and psychological effects of an RDD event are less well understood. No comprehensive standard has been established regarding what radiation limits would constitute a successful cleanup. Publications and released documentation written by the Al Qaeda organization indicate their understanding of the public unsettlement and possible economic consequences from an RDD attack. Dhiren Barot in 2006, Jose Padilla in 2007, and Glendon Crawford in August of this year were each convicted of attempting to develop and use a dirty bomb in New York City, Chicago, and elsewhere.

RDDs can be developed by a spectrum of adversaries from a relatively low capability lone wolf, such as these three individuals, to a highly capable and technically competent adversary, such as Aum Shinrikyo, who perpetrated the coordinated sarin attacks on the Tokyo subway system in 1995. The more technically capable an adversary is, the more likely they would be to find ways to spread the radioactive material over larger areas and at higher radioactive levels.

Since the 2000 UCLA [University of California, Los Angeles] study on RDD risk at the Ports of Los Angeles and Long Beach, many policies, programs, and systems have addressed the threat likelihood. This includes NRC [U.S. Nuclear Regulatory Commission] regulations for source security, the DOE [Department of Energy] Office of Radiological Security's domestic and foreign programs on radiological source security and recovery, and the DHS Domestic Nuclear Detection Office's Global Nuclear Detection Architecture to identify radioactive material outside of regulatory con-

trol. If a device is located prior to detonation, multiagency teams now exist for rapid response.

RDDs are unlikely to result in large immediate health effects beyond those caused by the explosive blast, although there may be some long-term effects to more exposed individuals. However, depending on the radionuclide involved, the economic consequences could be considerable.

If the radionuclide is difficult to remove from surfaces, as some are, the contaminated area could be off limits for months or even years. This would result in businesses within those areas being effectively shuttered and residents being relocated, semipermanently or permanently, while costly decontamination efforts are undertaken. Additionally, there would be interdependencies in the quarantined area between the residents and the businesses they patronize.

Since there is no comprehensive policy or standard for post-cleanup radiation levels, it is difficult to estimate the cost that would be directly associated with decontamination.

In summary, the RDD risk is real and multifaceted, and the U.S. Government has implemented a number of programs to increase the security of U.S. radiological materials and increase the difficulty of illicit movement of those materials, resulting in a reduced likelihood of an RDD attack. However, there is still significant uncertainty in our understanding of the costs that would accrue after such an event.

The development of policies and technical capabilities for effective cleanup to allow for resumption of normal operations following an RDD attack would constitute an important element of the multidimensional integrated solution for addressing the RDD threat.

Thank you.

Mr. HUNTER. Thank you, Dr. Potter. And you actually gave 30 seconds back from Dr. Canavan.

The next witness is Mr. Joe Lawless, the chairman of the Security Committee for the American Association of Port Authorities.

You are recognized.

Mr. LAWLESS. Thank you, Chairman Hunter, Ranking Member Garamendi, and distinguished members of the subcommittee. My name is Joseph Lawless. I am the director of maritime security at the Massachusetts Port Authority in Boston. I am here today on behalf of the American Association of Port Authorities, where I chair the Security Committee.

AAPA is the unified and collective voice of the seaport industry in the Americas. AAPA empowers port authorities, maritime industry partners, and service providers to serve their global customers and create economic and social value for their communities. Our activities, resources, and partnerships connect, inform, and unify seaport leaders and maritime professionals in all segments of the industry around the Western Hemisphere.

Security is our top priority for all of our members, and this testimony I am giving today is on behalf of our U.S. members.

Securing our ports and communities from dirty bombs could not happen without strong partnerships. This means our ongoing relationships with port authorities, the Federal Government, specifically the Customs and Border Protection agency, the United States

Coast Guard, the FBI, shippers, port workers, and State and local law enforcement, who all play a vital role in identifying threats and combining security resources to coordinate if a dirty bomb were to arrive on the U.S. shores.

The threat of dirty bombs ending up in the hands of people who want to cause us harm in this country was underscored recently by accounts of a disrupted illicit smuggling operation. It was reported that over the last 5 years there have been at least four attempts by criminals in Eastern Europe to sell radioactive materials to Middle Eastern extremists. If any of these smuggling plots were successful, these radioactive materials could have been used to construct a dirty bomb that could be ultimately used against us. The concern is that terrorists could exploit the maritime transportation system to convey a dirty bomb into this country.

Stopping dirty bombs before they reach our shores is a priority, but we must have an effective system of detecting dirty bombs if they were to make it to our shores. A fully funded and staffed Customs and Border Protection agency is the first step in fighting the threat of dirty bombs. CBP officers meet the ships at all ports of entry to check the manifests and utilize radiation portal monitors.

CBP and ports rely upon the RPMs to detect dirty bombs in containerized cargo shipped into this country. RPMs are detection devices that provide CBP with a passive, nonintrusive process to screen trucks and other movements of freight for the presence of nuclear and radiological materials. They are mandated in the SAFE Port Act of 2006, and the 22 largest ports by volume must have RPMs and all containers must be screened for radiation.

Almost 10 years have passed since the RPMs were mandated. However, a decade into this program questions have been raised regarding who pays for the maintenance of the RPMs, who is responsible for paying for new portals during port expansion, and what is the long-term obligation for the next generation of RPMs. A DHS inspector general 2013 CBP "Radiation Portal Monitors at Seaports" report states that the initial estimates of deployed RPMs showed an average useful life expectancy of 10 years.

What we hear repeatedly from our port members is the lack of clarity in funding and administering the RPM program. It has become a real hindrance in how we protect our ports. We are fast coming to the end of the first generation of RPMs' life expectancy. Ports such as Tampa, Jacksonville, Long Beach, New York/New Jersey, and Mobile have all reported complicated discussions with their regional CBP officers on the ongoing responsibilities related to RPMs.

A recent example is the Port of Jacksonville, where CBP requested that Jacksonville assume financial responsibility for the RPM technology sustainment, hardware, software, and connectivity. This is significant given the complex and critical nature of these federally owned and currently maintained systems. Other ports are reporting similar disruptions in the RPM program. There is too much at stake for ports and CBP officers to have to engage in policy and funding negotiations. Congress and the administration must set a clear path on the RPM program.

RPM detection is a federally mandated program. CBP should request adequate Federal funding to purchase, install, and maintain

all RPM equipment at ports throughout the United States. If this is not feasible, then the Department of Homeland Security should consider the creation of a stand-alone priority within the FEMA [Federal Emergency Management Agency] Port Security Grant Program, titled "Radiation Detection Portal Monitors," or expand upon the CBRNE [chemical, biological, radiological, nuclear, and explosives] core capability to allow ports to request security grant funding in support of the purchase and installation of radiation detection portals.

Regarding the Port Security Grant Program, many port authorities have utilized the Port Security Grant Program to obtain radiological and nuclear detection equipment. Personal radiation detection devices that first responders wear on their belts, isotope identifiers that are used to determine the source of radiation alarms, and sophisticated backpack detection devices are some of the items acquired through the Port Security Grant Program. These items not only supplement CBP's efforts, but also enhance law enforcement's role in the Coast Guard's small vessel rad/nuc detection program.

I would urge Congress to restore the funding for the Port Security Grant Program to its original level and maintain the Port Security Grant Program as a stand-alone Department of Homeland Security grant program.

Additionally, we would encourage that whenever possible, the grants go directly to the ports so that our security facilities will have the necessary resources to fully implement their security programs.

In conclusion, we must provide law enforcement agencies, such as the CBP, and our port security directors with all the tools and resources necessary to succeed.

I appreciate the opportunity to testify here today, and I look forward to answering any questions that you might have. Thank you.

Mr. HUNTER. Thank you, Mr. Lawless.

The final witness on the second panel is Dr. Stephen Flynn, director of the Center for Resilience Studies with Northeastern University.

You are recognized, Dr. Flynn.

Mr. FLYNN. Thank you, Mr. Chairman. You are going to hear two back-to-back Boston accents here now coming at you.

I have been at this for about 30 years, first as a Coast Guard officer, retired from that Service, and now currently at Northeastern University where with the support of the MacArthur Foundation I am looking at the growing risk of managing the threat to our global supply chains via the risk of radioactive material as well as weapons of mass destruction. So I am honored to be here today.

Mr. Chairman, it is my assessment that the threat of a dirty bomb at a U.S. port remains a clear and present danger. Simply stated, current U.S. efforts are not up to the task of preventing a determined adversary from exploiting the global supply system and setting off a dirty bomb in a U.S. port.

If a dirty bomb was set off in a U.S. port it would not be so much of a weapon of mass destruction as it would be of one of mass disruption. There would be three immediate consequences associated with this attack.

First, there would be local deaths and injuries associated with the blast of the conventional explosives.

Second, there would be the environmental damage and extremely high cleanup costs. As Dr. Potter was laying out here, we don't have standards for actually coping with the aftermath.

And then third, there would be what I call the morning-after problem. That is, since there would be no way of determining where the compromise that led to the incident happened within the security system, we would have sort of two outcomes. One, the entire supply chain, all the transportation nodes and providers, would be presumed to be potentially a risk of potential follow-on attacks. Further, it would call into question all the existing container port security initiatives that the first panel talked about here today.

On March 28, 2006, nearly a decade ago, and this is my 29th time talking about these issues before Congress since 9/11, I outlined the following hypothetical scenario that had been informed by my own research as well as the insights provided by Gary Gilbert, who is the chairman of the Security Committee of Hutchison Port Holdings, the world's largest terminal operator. I included in that testimony before the Senate Permanent Subcommittee on Investigations the following scenario.

A container of athletic footwear from a name brand company is loaded at a manufacturing plant in Surabaya, Indonesia. The container doors are shut and the mechanical seal is put into the door pad-eyes. These designer sneakers are destined for retail stores in malls across America. The container and seal numbers are recorded at the factory. A local truck driver, in this case sympathetic to Al Qaeda, picks up the container. On the way to the port he turns into an alleyway and backs up the truck at a nondescript warehouse where a small team of operatives pry loose one of the door hinges to open the container so they can gain access to the shipment.

Some of the sneakers are removed, and in their place the operatives load a dirty bomb wrapped in lead shielding, which will defeat the radiation portal monitoring, and then they refasten the door. The driver then takes the container, now loaded with a dirty bomb, to the port of Surabaya, where it is loaded on a coastal feeder ship carrying about 300 containers for a voyage to Jakarta. In Jakarta the container is transferred to an Inter-Asia ship, typically carrying 1,200 to 1,500 containers, to the Port of Singapore or the Port of Hong Kong. In this case, the ship goes to Hong Kong, where it is loaded on a super-container ship that carries 5,000 to 8,000 containers for the trans-Pacific voyage.

The container is then off-loaded in Vancouver, British Columbia. It is then loaded directly on to a Canadian Pacific railcar, where it is shipped to a rail yard in Chicago. Because the dirty bomb is shielded in lead, the radiation portals currently deployed along the U.S.-Canadian border do not detect it. When the container reaches its distribution center in the Chicago area, a triggering device attached to the door sets the bomb off.

Now, this scenario remains as realistic today as it was in 2006, because it exploits a longstanding vulnerability of the global supply system that still remains unaddressed: The ability of smugglers to potentially target a containerized shipment while it is being trans-

ported by a local truck from the factory or logistics center where it originates to the port where it's loaded aboard a vessel.

Now, once a truck leaves a factory, as a practical matter there are few controls in place for preventing a shipment from being diverted before it arrives at a port, particularly if the driver has been recruited, bribed, or intimidated into cooperating with a terrorist group intent on placing a dirty bomb into the container.

The container doors are typically "secured" with a numbered bolt seal that can be purchased in volume for about $1.50. But even if the bolt seal is left in place, as my scenario laid out, the door hinges can be removed or the container's relatively thin-metal skin can be breached so they can put the bomb in the box.

Now, I speculated that the hypothetical terrorist group would purposely target a container from a known shipper. I did this for two reasons. First, it can count on the fact that it is extremely unlikely that CBP will subject the container to any physical security as it originated from a well-established company. We have heard about the risk management system. And if it has no past record of smuggling, there is virtually no chance it will hit anybody's radar screen as a container to be checked.

Such a shipment from a trusted source would be deemed to be low-risk and as such not identified for an overseas port-of-loading inspection or an inspection in Vancouver when it is off-loaded to a U.S. bound train.

Second, by exploiting the container from a known shipper, the terrorist group can be confident they can generate the maximum amount of fear that all containers previously viewed low-risk now be judged as potentially high-risk. Fanned by the inevitable sensational media coverage, Governors, mayors, and the American people would place no faith in the entire risk management regime erected since 9/11.

I want to emphasize that this is why potentially a thoughtful adversary would put a dirty bomb in a box versus in a small boat. It is because the goal is not to get the bomb into the United States, it is to disrupt the global supply chain system by how we would respond in its aftermath. What we see here is that if we are suddenly spooked, there is a bomb in a bomb or there are other bombs in boxes, we basically would freeze the system to sort it out, not just one port closure, but almost certainly all port closures.

Then we have a challenge. We can't check the boxes until they are off-loaded, but the only way we can check them is if they are off-loaded. This catch-22 translates into ships queuing up in Anchorage outside our ports.

Overseas you can't just basically freeze the system. You are not going to send new ships into the U.S. if it is already backed up. You can't receive new boxes from trains and trucks. So essentially within 10 days to 2 weeks, the entire global intermodal transportation system goes into gridlock. The impact of that is disruption of our global commerce on a huge scale.

So what would we do? The real threat essentially is not so much the attack or the local harm for the port community, as significant as that is likely to be. It is the risk of mass disruption to international commerce that would follow from such an attack.

So two steps I outline in my testimony. The U.S. Government needs to shift its interests from one that focuses primarily on policing U.S.-bound cargo to one that advances the overall security resilience of the global supply system at large. There is compelling rationale for doing this. Everybody is signed up to trying to prevent the proliferation of weapons and materials around the planet. Specifically, all countries have signed on to U.N. Security Council Resolution 1540 that requires that nations take actions to detect and intercept outbound shipments of illicit nuclear and radiological materials. We have the international rationale. Let's get on with this at a global scale.

Secondly, the U.S. Government really needs to focus on enlisting the active participation of private industry that owns and operates the port terminals and transportation conveyances that move supply chains. They have a rationale to do this. This is a significant business continuity enterprise resilience imperative. As such, the conventional wisdom that security is basically a public sector responsibility is wrong. It is primarily a public sector responsibility to work this, but the private sector has a critical role to play.

The foiled October 2010 bomb plot involving explosives hidden in printer cartridges shipped from Yemen make the case. In the aftermath of that we saw the aircargo industry working with U.S. and European authorities to significantly step up the scrutiny of aircargo.

The maritime transportation system, in short, is a highly concentrated system with a few large port terminal operators and ocean carriers responsible for handling the vast majority of global cargo. With support from the U.S. Government and other authorities, these companies could potentially take on a leadership role for deploying the technologies and tools on a global scale by providing a near real-time visibility and accountability for contents and location of all cargo.

What they would need is the means to recover the associated costs through a fee-for-service requirement that is borne by importers and exporters. The estimated cost of putting nonintrusive inspection and terminal operations around the world ranges from $3 billion to $5 billion. Given that there are millions of containers moving through, we are talking about a $10 to $15 per-box cost largely to do this, or less than the security surcharge I had from flying from Boston to Washington for this hearing today.

In conclusion, Mr. Chairman, the risk of an adversary exploiting the global supply system to import a dirty bomb at a U.S. port remains clear and present. The disruption that such an attack would generate goes well beyond the local port. It would ripple through the entire maritime transportation system. It would be disastrous for global trade.

Accordingly, the stakes for the United States national security and economic security could not be higher. There is an urgent need to significantly bolster and build upon the many post-9/11 initiatives which aim to improve the security of the maritime transportation system. In the end, these global networks require trust to operate. We have got to work on ensuring we can survive that trust in the event of a dirty bomb going off in a port.

Thanks so much.

Mr. HUNTER. Thank you, Doctor.

And thanks to my colleagues for sticking around too. I am just going to ask a quick question and then going to pass it off so everybody else can get a question in before we have to leave.

Dr. Canavan, I guess the question is this. If you are going to have a nuclear weapon come in, dirty or not, it is going to be shielded. If it is not, I would recommend to our enemies that they shield it, otherwise it will be easier to see. So I would think that some smart people would shield it. Can you still see it?

Mr. CANAVAN. Yes, sir, good question. I cover that a little bit in my testimony. Bombs are not easily shielded from inspection by neutrons. As I said, if you keep the neutrons fast enough—that is, with high enough energy—they are not affected by absorbers. Neutrons can go through a whole ship without hardly slowing down.

The tricky part is what are called moderators, things that reduce the energy of the neutrons. If a bomb was packed in a bunch of moderator material, carbon or something like that that can slow neutrons, enough of it could slow the neutrons down to where not enough of them would penetrate into the core to give you a good nuclear signature. It is not a precise number, but a foot or so of carbon outside the device might effect that sort of slowing down.

But there are two things that you have to consider. One is that by the time you have a few feet of carbon on either side of the device you block the whole TEU, the container that it is in, and that in itself would be a signal that someone had tried to hide it. It is not an easy thing to do.

The other thing is, it is a technical point, but when neutrons bounce off of a moderator like carbon they produce a spectrum of bands of energy that are easily detectable. The spacing of the energy bands are a good indicator of what kind of moderator the person is using to try to beat you, and the number of those bands tell you how thick the moderator is.

That is the game that they would play. It is not an easy game for the adversary. That is all I can say.

Mr. HUNTER. There is a company that I know of called Decision Sciences that actually is able to sense nuclear stuff inside of really thick lead, but you have to be in their system, meaning that you can't walk around and scan stuff. It has got to be within basically one of those drive-through systems to do this. And it takes more than just a drive through, it takes a couple of seconds.

Mr. CANAVAN. Decision Sciences uses muons. They do not select nuclear material, just mass. Neutrons go through anything. They particularly like to go through steel and lead. So ordinary shielding, which is very effective for dirty bombs and even uranium in its natural state emitting radiation is not very effective against fast neutrons. Somebody has to really, really go out of their way with a lot of shielding to try to knock the signal down. Sorry.

Mr. HUNTER. But these handheld detectors, they wouldn't sense something if it was in carbon or lead. It would take an actual scanning system to do that, right? The handheld CBP detectors, they are not going to detect stuff if it is in a TEU?

Mr. CANAVAN. Correct. Handheld detectors are defeated by a modest amount of shielding. The trick with neutron detection is that you inject a signal which is magnified by the target itself to

a detectable number of neutrons coming back out. And so you are stimulating very gently the fissile material to produce a signal that would not be there in the case if you didn't stimulate it.

Mr. HUNTER. And the only way to do that is through one of these drive-through systems, meaning none of this is going to happen by a handheld device that someone is holding walking around or a belt device.

Mr. CANAVAN. Correct. The spontaneous signal is too weak for them to detect.

Mr. HUNTER. All of this only comes, even the best we can do, through, like, a drive-through scanning system, right, where you can spray it with neutrons and then have that read on the other side, which takes a system.

Mr. CANAVAN. Neutrons could act in a drive-through, but they could also operate in other modes discussed below. There is no free lunch. You do have to produce the neutrons, but neutrons are not very hard to produce. The trick is knowing that you have to both put them where you want them and then collect them in a smart way.

Mr. HUNTER. Thank you.

And I am going to yield, because I am out of time. Mr. Garamendi is recognized.

Mr. GARAMENDI. Apparently the bottom line on your testimony is that a compact fast neutron inspection can work. We are not presently deploying those. Is that correct?

Mr. CANAVAN. Correct. As I said, we kind of went off on a tangent that was not very productive. And it has only been sitting around and scratching my head for a long time sort of gave me the idea. As Dr. Teller, my old professor, always used to tell me, the hardest thing about doing something is unlearning what you thought——

Mr. GARAMENDI. We are going to move this right along because we are out of time.

Dr. Potter, you seem to think that domestic steps need to be taken, cesium chloride specifically?

Mr. POTTER. A National Academy study was done, some years ago now, pointing out the need to protect cesium chloride sources throughout the United States, yes.

Mr. GARAMENDI. So you drew our attention to that issue, and presumably we will avoid dealing with that problem.

Mr. POTTER. Uh-huh.

Mr. GARAMENDI. Which is not a good solution.

And finally, Mr. Lawless, it comes down to money, doesn't it? Who is going to pay for the detectors, the kind Mr. Canavan is talking about, domestically with cesium chloride? How much money do you need to put these detectors and to maintain them?

Mr. LAWLESS. Well, that is a difficult question to answer. I would suggest that the Government fund these research projects, like these drive-through portals, that we would see that could detect neurons and gamma at the same time. We are invested at my particular port working with DNDO and a company to develop a state-of-the-art detection system in the Port of Boston.

But there is definitely money needed to fund these programs. There has to be clarity on who is paying for these systems. They

are federally mandated systems. And the ports believe that the Federal Government should be paying CBP and DNDO to fund these projects.

Mr. GARAMENDI. Dr. Flynn is willing to put $10 to $15 on each container. I assume you have an opinion on that. Yes? No?

Mr. LAWLESS. Yes.

Mr. GARAMENDI. All right. And I would just go back to where I started this, in that we make choices around here, and we are looking to spend $3.5 billion for a missile defense system for the east coast to deal with Iran nuclear weapons, which presumably aren't going to be available for some decades.

Thank you, Mr. Chairman. I yield back.

Mr. HUNTER. Thank the gentleman.

Ms. Hahn is recognized.

Ms. HAHN. Thank you.

Dr. Flynn, thank you for being here today. I have followed your work and read a lot of what you have written. Again, I represent the Port of Los Angeles and I am always very concerned. As you said, the Container Security Initiative scans less than 1 percent of U.S.-bound cargo. Do you believe that scanning at the point of origin is effective, 100 percent effective, or should we be investing more in scanning at our domestic ports?

Mr. FLYNN. Well, this is an issue where the stakes are so high we should be looking at dealing with this across the board. So relative to where we put resources, this really ranks right up there, I think, given the consequence we laid out. And I have spent a good bit of time in the Port of L.A. and Long Beach and you really get the sense of scale about what is going on here.

And what the problem would be in this dirty bomb scenario, where if we spread all that stuff around how would you work in that port, as well as, of course, neighbors who live in San Pedro and so forth? This would be a real challenge.

So in the face of this here there is opportunity at the port of loading, even at the largest terminals, to scan cargo. Now, what that would do is it should be baked into the terminal operations. Just as the radiation portals are here even when you leave the terminal, we would like to ideally have that when people drive into the terminal. And you can't do it for just U.S., you have to do it for everything. And that is where there is counterproliferation value to doing this, because most of the stuff we worry about proliferation is going not to the United States, but is going around. And to the extent that is a national security imperative, trying to get visibility into what moves through the intermodal transportation system should be a key.

So let's be clear right now with the numbers: 2013, the numbers of CBP inspections overseas in the then-58 ports around the world was 103,000. If you divide that by 365 days and 58 ports, we are talking 5 containers per port, per day are being examined overseas under the CSI system. OK, it is five a day. And if you have been to places like Singapore or Shanghai or others, I mean, it may be up a little bit.

Why is that? It is because the current approach is we are going to identify the risk and actually go pluck the box and take it to a Government inspection facility. If you bake it into the operation of

the terminal you would collect this in real time. It doesn't mean you have to look at images every time. What you would do is would get those and use your risk-based approach to do it, but you would have a much greater degree of confidence about deterring this risk, but also ultimately finding things when they go wrong to intercept them, or worse case even isolating the incident afterwards so you don't shut down the whole system.

So there is just so much that can be done, should be done, that is not being done.

Ms. HAHN. Thank you. I appreciate the warning. And as you commented, which I also did in the first panel, was the threat to our global economy is significant, particularly if something happened at Long Beach and Los Angeles. We know what that impact would have on not just our national economy, but the global economy.

So I was going to ask one more, Dr. Canavan. I mean, I think the biggest issue that everyone tells me why we can't have 100 percent scanning is that in some way that would impede, slow down commerce and we just can't afford that. And by the way, I do have a bill that would provide grants to two ports in this country that would voluntarily decide to implement 100 percent scanning with the technology that we have available, just to I sort of want to prove everybody wrong, that actually we can do this and not impede commerce in a way that would really impact the economy.

But, Dr. Canavan, is there technology, of that that you spoke about, which one of those technologies could work and also not impede commerce?

Mr. CANAVAN. Well, there are two—there is one technology I talk about and that is interrogation with neutrons. I think it would fill the requirements that you are setting down there. There are these big cranes that move containers around. I would like to put a little source on one leg of the crane and the detector on the other, so while it is moving them around there would be plenty of time to inspect them. It does its inspection in seconds or milliseconds. It is very fast.

The other approach would be to mount the source and detector on the bulkheads of the ship, sort of one per canister, so that you could keep track of what happens to that canister the whole time it is out at sea.

I think you could do that, but I haven't proved it, ma'am. I have tried to show that the physics is OK.

Ms. HAHN. Thank you very much.

Mr. HUNTER. Ms. Brownley is recognized.

Ms. BROWNLEY. Thank you, Mr. Chairman.

And, Dr. Flynn, your points and your testimony I think were well taken, that it is not an attack just on U.S. soil, but an attack on trade and interrupting goods movement in our country.

And I am just wondering if you have very specific recommendations for how individual ports and the businesses within those ports can really prepare for—or prepare for a contingency plan in the event that we did have an attack, and also specific recommendations for governmental agencies and what they should be doing for contingency as well.

Mr. FLYNN. I mean, I really applaud the question and the focus, because unless we assume that this is a zero chance that this will happen that we will have a nuclear event, we should have a plan. That is something we can do. It is not a huge cost issue. It is a heavy coordination issue and a collaboration issue.

The core challenge is that, as I also laid out in my testimony, this is a global system sort of running on steroids. And so if you disrupt it at any point, increasingly it cascades across the system. So it is a lot of choreography.

Right now the U.S. Government has no plan for how to deal with this beyond the U.S. borders. There is a global strategy the President put out. I think it is the world's thinnest strategy, it is four and a half pages. It basically says we should have a plan, but nobody actually has executed on that.

And thinking through that, so some specifics. Clearly it is raising the awareness about what this event would look like and then mechanics about, OK, how do we deal with the immediacy of the dirty bomb? What is safe? I mean, this is something a community can't solve because the U.S. Government has to set what standards are for safety in terms of putting people back into that community.

But the coordination is really heavily between the industry that runs the system and the port authorities and the local authorities and the governmental authorities who manage the system. There we have very limited visibility about how it works. And what makes this, I think, a unique and challenging issue for critical infrastructure, the maritime transportation system, is that 90-plus percent of it is internationally owned, it is not U.S.-owned, and we have to coordinate therefore with those key players.

But the opportunity is, it is a concentrated industry. There are roughly five terminal operators that move about 80 percent of all the goods to the United States. They are in ports all over the world. You don't have to go to 180 nations, you go to 5 companies. There are basically 20 ocean carriers that matter. You can work with 20 CEOs.

What we have been doing is looking at this as a Government-to-Government issue or local government issue when it really is an international private system that we have to have a capability.

In our financial meltdown in 2008 we had central bankers who could manage the morning after. It was messy, but we had a system. We have no such system for managing a major disruptive event, and that is something that I think transcends anything that these agencies who are here this morning their job is to do, but it is a high order national security and economic security issue for us to wrestle with.

Ms. BROWNLEY. And you had mentioned that we should be listening to industry and businesses clearly in terms of what they believe are the right—what is the right direction and the right plans for contingency. And do you have any idea what they, I guess, would suggest? I mean, in the earlier testimony they said if we had an incident we would just—industry would just respond and that would be the contingency plan.

Mr. FLYNN. Well, I have worked closely on that and I have talked to the CEOs of the largest terminal operators. If there is a plan, they are willing to engage on the plan. This is a business con-

tinuity issue for them. If there is a cost-recovery mechanism for deploying equipment, they are willing to do that.

I had two colleagues and I that work out of the Wharton School looking at two choices, the one we have right now where we would select a box out of a container and send it to be inspected at very small percentages or one where you scan all of them. The terminal operator we worked with said, "It is easier for me to scan them all then for you to come into my yard, packed six high, and grab two to get the one and take it around."

So in some places it turns out doing more is easier. The economics work better. OK? And in other places, in sleepier, slower places, you are probably not going to have that same level of buy-in and then you probably use a different approach. I mean, there is not going to be a one-size-fits-all. But when you have a conversation with industry it comes out a lot different than maybe the one you have when you do a Government-to-Government one.

And here it is an engineering problem, it is an operational problem with some technical complexity. But it is not insoluble. We should not be throwing our hands up in the air and going let's just hope it never happens. Shame on us when it does happen.

Ms. BROWNLEY. Thank you very much.

And I will yield back, Mr. Chairman.

Mr. HUNTER. I thank the gentlelady.

We have run out of Members. By the way, this was not a bad showing for today. Usually it is just me and John sitting here. So at least we had some people.

But thank you very much for what you all do for the country and for industry and thanks for being here.

With that, the hearing is adjourned.

[Whereupon, at 12:28 p.m., the subcommittee was adjourned.]

U.S. Department of Homeland Security
United States Coast Guard

Commandant
United States Coast Guard

2100 Second Street, S.W.
Washington, DC 20593-0001
Staff Symbol: CG-0921
Phone: (202) 372-3500
FAX: (202) 372-2311

TESTIMONY OF
REAR ADMIRAL PETER J. BROWN
ASSISTANT COMMANDANT FOR RESPONSE POLICY

BEFORE THE
HOUSE COAST GUARD AND MARITIME TRANSPORTATION SUBCOMMITTEE

OCTOBER 27, 2015

Introduction

Good morning Chairman Hunter, Ranking Member Garamendi, and distinguished Members of the Subcommittee. I am honored to be here today to discuss the Coast Guard's role in the prevention of and response to the arrival of a radiological dispersion device (also called a "dirty bomb") in a U.S. port.

In my role as Assistant Commandant for Response Policy, I oversee the development of Coast Guard response doctrine and policy; this includes the response to incidents of terrorism in the maritime domain.

The U.S. maritime domain is vast and challenging in its scope and diversity and is not limited to the nation's shorelines. It encompasses the expanse of our ports and coastal waters, our Territorial Sea, Contiguous Zone, and our Exclusive Economic Zone (EEZ). Securing our maritime borders requires multi-faceted authorities, capabilities, competencies and partnerships. Because of its broad reach in the maritime domain, the Coast Guard plays a role in the whole of the government effort to mitigate the risks posed by the transportation of a dirty bomb to a U.S. port during all phases of the risk mitigation spectrum: from prevention and detection - to protection and response - to recovery.

Through a layered security approach, the Coast Guard pushes border security well beyond the Nation's shoreline and EEZ by fostering strategic relationships with partner nations to detect, deter, and counter threats as early and as far from U.S. shores as possible in order to prevent an attack on the homeland.

Prevention

The Coast Guard's effort to prevent dirty bombs from nearing U.S. ports and shores begins overseas, with robust international partnerships that provide access at maritime points of origin.

The Coast Guard conducts foreign port assessments and leverages the International Maritime Organization's (IMO) International Ship and Port Facility Security (ISPS) Code to assess effectiveness of security and antiterrorism measures in foreign ports. Through the International Port Security Program, the Coast Guard performs overseas port assessments to determine the effectiveness of security and antiterrorism measures exhibited by foreign trading partners.

Since the inception of the ISPS Program in 2004, Coast Guard personnel have visited more than 150 countries and approximately 1,200 port facilities. These countries generally receive biennial assessments to verify continued compliance with the ISPS Code. Vessels arriving in foreign ports that are not compliant with ISPS Code standards are required to take additional security precautions while in those ports. They may also be boarded by the Coast Guard before being allowed entry to U.S. ports, and in some cases are refused entry into the United States.

To more effectively counter maritime threats in the offshore region and throughout the Western Hemisphere, the Coast Guard maintains more than 40 maritime bilateral law enforcement agreements and arrangements with partner nations. The Coast Guard is also the U.S. Competent Authority for 11 bilateral Proliferation Security Initiative ship boarding agreements, which facilitate international cooperation to board vessels at sea suspected of carrying illicit shipments of weapons of mass destruction, their delivery systems, or related materials by establishing procedures to board and search such vessels in international waters. These agreements and arrangements facilitate coordination of operations and the forward deployment of boats, cutters, aircraft, and personnel to deter and counter threats as close to their origin as possible.

To foster international cooperation and build partner capacity, Coast Guard personnel are posted at several embassies throughout the world and at all Department of Defense Combatant Commands. These individuals develop strategic relationships with partner nation maritime forces that facilitate real-time operations coordination and enduring maritime security cooperation.

The Coast Guard's membership within the intelligence community provides global situational awareness, analysis, and interagency collaboration opportunities with various counterterrorism components, including the Central Intelligence Agency, National Counterterrorism Center, the Federal Bureau of Investigation (FBI), and the Department of Homeland Security's (DHS) Office of Intelligence and Analysis, among others. The Coast Guard enjoys unique access through liaison positions, the Defense Attaché program, the Joint Duty Assignment program, and the Coast Guard Cryptological Group. This access provides insight into counterterrorism events where the Coast Guard is able to bring expertise and focus on maritime-related situations.

The Coast Guard's authorities through the Maritime Transportation Security Act of 2002 (Pub. L. No. 107-295) (MTSA) provide a regime of security plan compliance and inspections for both maritime facilities and vessels; this reduces the Nation's vulnerability to terrorist attacks in or involving the ports. In U.S. ports, Coast Guard Captains of the Port (COTP) are designated as the Federal Maritime Security Coordinators (FMSC). In this role, COTPs lead the Nation's 43 Area Maritime Security Committees (AMSC) and oversee the development, regular review, and annual exercise of their respective Area Maritime Security Plans. AMSCs assist and advise the FMSC in the maintenance of a coordination and communication framework to identify risks and vulnerabilities in and around ports.

Additionally, AMSCs coordinate resources to prevent, protect against, respond to, and recover from Transportation Security Incidents. AMSCs have developed strong working partnerships between all levels of government and private industry stakeholders.

Detection

Building on prevention efforts, the Coast Guard brings both agility and mobility to the Nation's detection regime with its ability to deliver detection capability anywhere in the maritime domain.

The Coast Guard conducts over 400 routine inspections and general law enforcement boardings every day to ensure that vessels comply with international maritime law and safety standards, applicable U.S. law and regulations, and any control procedures required to access the Nation's ports. Coast Guard personnel that visit boats, vessels, or regulated facilities carry a basic detection device designed to alert the user to the presence of radiation.

In 2004, the Coast Guard developed and implemented a Coast Guard-wide Maritime Radiation Detection program and has since maintained a close relationship with the DHS Domestic Nuclear Detection Office (DNDO) to standardize equipment and enhance the national capacity for detection with layered levels of organic capability. The Coast Guard actively participates in DNDO strategic joint radiation detection acquisition programs that seek to standardize or increase compatibility of radiation detection platforms among the key components, including the Coast Guard, Customs and Border Protection (CBP), and the Transportation Security Administration (TSA). The Coast Guard also participates in inter-component training sponsored by DNDO. The result of joint acquisitions and training is successful, ongoing Coast Guard support to CBP seaport inspections as well as to TSA Visible Intermodal Prevention and Response Teams at major intermodal and passenger ports.

All operational Coast Guard units such as Sectors, Deployable Specialized Forces, Cutters, and Boat Stations possess a radiological detection capability that can identify specific isotopes, distinguish between man-made and natural sources, and can "reach back" to interagency experts for technical assistance. The Maritime Security Response Team (MSRT) provides the nation with maritime capability for nuclear and radiological detection, identification, personnel protection, and self-decontamination in either routine or hostile situations. MSRT capabilities are designed and implemented to integrate with other interagency or DOD response forces.

Complementing an array of personal and shipboard detection devices, the Coast Guard conducts vessel screening at the national and tactical levels. At the national level, through the Intelligence Coordination Center's Coastwatch Branch, which is co-located with CBP at the National Targeting Center, the Coast Guard screens ship, crew, and passenger information for all vessels required to submit a Notice of Arrival (NOA) prior to entering a U.S. port. In 2014, Coastwatch screened approximately 124,000 NOAs and 32.7 million crew and passenger records. Additionally, through partnership with CBP, the Coast Guard has expanded access to counter-terrorism, law enforcement, and immigration databases, which has led to greater information sharing and more effective security operations. At the tactical level, each of the Coast Guard's Area Commanders receives support from a Maritime Intelligence Fusion Center (MIFC), which screens commercial vessels operating in its area of responsibility for unique indicators.

The MIFCs focus on screening characteristics associated with the vessels itself, such as ownership, associations, cargo, and previous activity. Screening results are disseminated through Regional Coordinating Mechanisms (ReCoMs) to interagency partners to evaluate and take action on any potential risks.

Response

The Coast Guard's response to a dirty bomb discovery would be part of a coordinated interagency effort in order to bring the most appropriate national resources and capabilities to bear.

The response to a radiation detection alarm begins with determining the source and type of material, which is then correlated with the legitimate cargo listed in the ship's manifest and the NOA. In these instances, the Coast Guard collaborates closely with CBP Laboratory Scientific Services to identify the specific isotope present and to otherwise determine if a threat exists.

If a dirty bomb is suspected or identified within a port, interagency Maritime Operational Threat Response (MOTR) protocols would be employed to provide coordinated interagency actions to achieve a solution. In such a scenario, the Coast Guard COTP would apply existing broad security authority to direct vessel movements and control port access until the issue was resolved. The COTP could establish and enforce maritime safety or security zones within the port to protect people and infrastructure - or could issue orders directing any particular vessel to operate or anchor in a specified manner. Coast Guard vessels, stations, or other shore-based forces such as Maritime Safety and Security Teams (MSSTs) or the MSRT would be deployed to enforce security zones, creating a visible deterrence and a potential disruption to attack planning.

The Coast Guard's MSRT is also equipped to directly respond to such maritime threats. In the case of a suspected dirty bomb, the MSRT can provide a tactical search capability to detect, identify, and classify such a device. The MSRT is capable of operating in a contaminated environment while engaging hostile threats in order to locate and secure a dirty bomb; it does not, however have the capability to disarm or "render safe" a device. The MSRT is a force multiplier for ambiguous or multiple threat scenarios in cases where DOD or FBI assets may also be responding.

Recovery

During the recovery phase of a dirty bomb detonation, the Coast Guard would be focused on the safe restoration of commerce, as quickly as possible.

Under the Nuclear/Radiological Incident Annex of the National Response Framework, the Coast Guard serves as the "coordinating agency" for incidents that occur in the coastal zone. The Coast Guard works with other agencies to determine how best to cooperatively respond consistent with the National Contingency Plan model.

Because of our unique maritime jurisdiction and capabilities, the Coast Guard can provide security, command and control, transportation and support to other agencies that need to operate in the maritime domain. The FBI is the lead federal agency for criminal investigations of all terrorist related incidents and must be contacted in any incident involving radiological materials.

The National Strike Force (NSF) includes the Strike Force Coordination Center and thePacific, Gulf and Atlantic Strike Teams. Each Strike Team has the capability to support the Federal On-Scene Coordinator in the event of a dirty bomb/radioactive material contamination to monitor and assess the situation. The NSF can operate in a radiological environment; conduct radiation surveys; monitor personnel exposure; conduct site, personnel, and equipment decontamination operations; and monitor and supervise contractors in a radiological environment.

A dirty bomb detonation in a port could lead to disruption or suspension of port activities. The scope would depend on the affected port(s) but could have significant national economic impacts. To enhance port recovery efforts in the event of an incident, a Coast Guard Maritime Transportation System Recovery Unit (MTSRU) may be established to prioritize backlogged shipping entering and leaving the port.

Conclusion

From our efforts to push out our maritime border and strengthen our international and domestic partnerships to our investments in cutter, boat and aircraft recapitalization, the Coast Guard continually adapts to evolving maritime border security threats while facilitating the safe flow of legitimate commerce. While a dirty bomb scenario would require a coordinated interagency effort, the Coast Guard's layered security strategy is well suited to address the broad range of offshore and coastal threats that could impact our national security and economic prosperity.

Thank you for the opportunity to testify today and thank you for your continued support of the United States Coast Guard. I would be pleased to answer your questions.

Testimony of
Huban A. Gowadia, Ph.D.
Director for the Domestic Nuclear Detection Office
U.S. Department of Homeland Security

Before the House of Representatives Committee on Transportation and Infrastructure
Subcommittee on Coast Guard and Maritime Transportation
October 27, 2015

Chairman Hunter, Ranking Member Garamendi and distinguished Members of the Subcommittee. Thank you for the opportunity to testify with my colleagues from the Department of Homeland Security (DHS) on the Domestic Nuclear Detection Office's (DNDO) efforts to prevent and respond to the arrival of a radiological device at our Nation's maritime ports.

Radiological and nuclear terrorism remains one of the greatest threats to our Nation's security. An attack with a radiological dispersal device, also known as a "dirty bomb," at a U.S. port would have profound and prolonged impacts to our Nation and the world.

Since its inception, DNDO has built essential partnerships, developed strategies, and deployed capabilities to detect and interdict radiological and nuclear threats posed to the homeland. Additionally, DNDO, in partnership with our interagency partners from the Departments of Defense (DoD), Energy (DOE), State (DoS), Justice (DOJ), and the Office of the Director of National Intelligence (ODNI), has advanced national technical nuclear forensics to trace nuclear and other radioactive materials back to their source. My testimony today focuses on work to strengthen the operational readiness of our maritime partners and efforts to improve the technical nuclear forensics capabilities of the U.S. government (USG).

In both nuclear detection and forensics, we rely on the critical triad of intelligence, law enforcement, and technology. Thus, to maximize our Nation's ability to detect and interdict threats in the maritime domain, it is imperative that we apply detection technologies in operations driven by intelligence indicators, and place them in the hands of well-trained law enforcement and public safety officials. The USG also must ensure that information from law enforcement, intelligence, and technical nuclear forensics is synthesized to identify the origin of the material or device and the perpetrators.

DNDO was established in 2005 by presidential directive and subsequently codified in the SAFE Port Act (P.L. 109-347) amending the Homeland Security Act of 2002. DNDO is responsible for the coordination of federal efforts to detect and protect against attempts to import, possess, store, develop, or transport nuclear or other radioactive materials out of regulatory control that may be used as weapons against the Nation. Necessarily, our efforts are collaborative with federal, state, local, tribal, territorial, and international partners, as well as with academia, the national laboratories, and industry. DNDO with its interagency partners coordinates the development and enhancement of the global nuclear detection architecture, which is a framework for detecting, analyzing, and reporting on nuclear and other radioactive materials that are out of regulatory control. DNDO is responsible for implementing the domestic portion of the global nuclear detection architecture. The architecture presents a layered, multi-faceted, defense-in-depth

framework to ensure prospective terrorists face multiple obstacles. Our goal is to prevent nuclear terrorism by making it a prohibitively difficult undertaking for the adversary.

Our efforts to secure the homeland from the threat of nuclear terrorism begin overseas. A *global* nuclear detection architecture relies largely on the decisions of 195 sovereign foreign partners to develop and enhance their own national and regional detection programs. To that end, DNDO, in close cooperation with the interagency and multilateral partners such as the International Atomic Energy Agency (IAEA), the Global Initiative to Combat Nuclear Terrorism (GICNT), and INTERPOL, promotes the development of national nuclear security detection architectures.

Further, programs implemented by our interagency partners seek to secure and reduce the available material abroad as well as assist partner nations with interdicting and deterring the possession and use of illicit materials and weapons. DOE's Office of Radiological Security provides a first line of defense by securing radioactive materials used for legitimate medical, industrial, and research purposes; removing and storing disused radioactive sources; and, where feasible, encouraging the use of non-isotopic alternative technologies that cannot be used as weapons. DOE's Nuclear Smuggling Detection and Deterrence program also contributes significantly to the capacity of partner countries to deter, detect, and interdict illicit trafficking of nuclear and radiological material across international borders and through the maritime shipping network by providing partner country governments fixed and mobile detection equipment and support to indigenously advance and sustain a nuclear detection architecture. DOE's efforts in these areas complement the DHS mission to protect the homeland by preventing terrorists and other criminal groups from accessing and using radioactive materials to carry out an attack.

To assist partner nations in their nuclear security endeavors, DNDO, working through the aforementioned international organizations, develops and shares guidance, best practices, and training courses. These efforts focus on foundational elements of detection architectures, such as planning, risk assessment, strategy development, legal and regulatory frameworks, and the integration of intelligence networks and law enforcement.

In acknowledgement of the serious nature of the threat, President Obama established a series of Nuclear Security Summits, beginning in 2010, as an international forum for improving nuclear security worldwide. Consistent with commitments made at these summits, nations are improving security at nuclear and radiological facilities, enhancing abilities to counter nuclear smuggling, and removing or disposing of nuclear materials. Although less nuclear and radiological material is available for use by terrorists due to these efforts, much work remains and the threat requires our constant attention.

The 2016 Nuclear Security Summit is anticipated to continue discussions to improve nuclear security efforts to deter, detect, and disrupt attempts at nuclear terrorism. As part of the Department's endeavor to address the congressional mandate to scan 100% of U.S.-bound maritime cargo containers overseas, DHS, DOE, and other USG representatives will participate in the Nuclear Security Summit Maritime Security Workshop in November 2015, which will specifically address radiation detection in the maritime environment. Any recommendations developed will be presented at the 2016 summit.

The summits, along with the aforementioned international efforts, contribute to building a multi-faceted, multi-layered approach for detection so nuclear and other radioactive material out of regulatory control can be interdicted before it is transported to the United States.

The layered approach to countering nuclear terrorism continues at our borders. To fulfill DNDO's responsibility to implement the domestic portion of the global nuclear detection architecture we work with DHS operational colleagues to develop and deploy detection technologies and state and local agencies to establish and enhance their detection capabilities. DNDO procures large-scale fixed radiation detection systems and small mobile devices for employment at our ports of entry, along our land and maritime borders, and in the interior of the United States. As such, we collaborate with the U.S. Coast Guard (USCG), U.S. Customs & Border Protection (CBP), and the Transportation Security Administration (TSA).

To bolster detection capabilities at our maritime borders, DNDO has procured portable radiation detectors for the USCG so that all boarding teams are equipped with mobile devices to scan for the presence of radiation. To increase the probability of detecting threats posed by small vessels, DNDO has also acquired capabilities for use by USCG and CBP vessels to scan such vessels before they reach our shores. To facilitate the scanning of inbound cargo containers, DNDO, in collaboration with CBP, has also procured and deployed radiation portal monitors and radioisotope identification devices for use at the ports of entry. As a result, today, almost 100% of all incoming maritime containerized cargo is scanned for radiological and nuclear threats at our seaports.

At the same time, we continue to enhance our fielded capabilities. To improve the performance of radiation portal monitors and gain efficiency at land and maritime ports of entry, CBP and DNDO worked closely on implementing an approach to reduce the number of nuisance alarms. Radiation portal monitors routinely detect benign radioactive materials in the stream of commerce, resulting in a significant operational burden for CBP field officers who must resolve these alarms. CBP and DNDO worked closely to implement a new algorithm, reducing nuisance alarms (by 74% on average) without sacrificing detector performance against threat materials. The reduction in alarm rates and decrease in secondary security inspections has enabled officers in the field to redirect their attention to other high priority law enforcement duties.

To advance technology to detect threats, DNDO performs accelerated development, characterization, and demonstration of leading-edge technologies. One such effort is the Nuclear and Radiological Imaging Platform project, where DNDO is developing and evaluating emerging technologies to detect shielded materials while clearing benign conveyances at land and maritime ports. We are also collaborating with CBP's Laboratories and Scientific Services to use machine learning to further reduce the number of nuisance alarms in radiation portal monitors deployed to ports. In addition, we are working with the Massachusetts Port Authority, DHS Science and Technology's Border and Maritime Security Division, and the United Kingdom's Home Office to develop and evaluate the next generation non-intrusive inspection imaging equipment. The technology will be evaluated in the Port of Boston next year and, if successful, will demonstrate a next generation integrated system capable of detecting both nuclear material and contraband.

While technology is critical to detection, building operational capacity through training, exercises, and cross-jurisdictional protocols is integral to securing our maritime borders. DNDO

works with federal, state, local, tribal, and territorial agencies to build flexible, multi-layered capabilities that can be integrated into a unified response when intelligence or information indicates a credible radiological or nuclear threat.

DNDO also provides program assistance to aid maritime partners in developing radiological and nuclear detection programs based on lessons learned in the West Coast Maritime Pilot, a collaborative effort with partners from Puget Sound, WA, and the Port of San Diego, CA. Under the leadership of the Area Maritime Security Committees, the pilot successfully established efficient, risk-informed regional detection programs focused on detecting and interdicting threats posed by small vessels in the maritime pathway. Lessons from this pilot have also shaped DOE's Maritime Vectors Program, which is an element of the DOE/NNSA Defense Nuclear Nonproliferation Office of Nuclear Smuggling Detection and Deterrence that seeks to deter, detect and interdict international smuggling of nuclear materials via unregulated maritime traffic. Today, DNDO's maritime assistance program works with Area Maritime Security Committees to develop regional Concepts of Operations and Standard Operating Procedures, provides information on detection equipment needed to support the same, and provides guidance on training and exercise plans.

To further our domestic capabilities to detect and interdict nuclear and other radioactive material out of regulatory control, DNDO is currently engaged with all 50 states and 33 of the USCG's Area Maritime Security Committees. Since intelligence and information sharing is integral for our collective success, DNDO efforts are focused on bringing together federal, state, local, tribal, and territorial partners at the outset. DNDO and DHS's Office of Intelligence & Analysis, along with our federal interagency partners at the Federal Bureau of Investigation (FBI) and the National Counterterrorism Center (NCTC), ensure that state and local partners have the information and tools necessary to address evolving threats. State and major urban area fusion centers, State Emergency Control Centers, and the FBI Joint Terrorism Task Forces (JTTFs) provide the necessary information exchange pathways. In the event of an emergency, this connected system provides federal, state, local, tribal, and territorial personnel with the ability to exchange sensitive information in a timely and secure manner.

To enhance situational awareness of radiological and nuclear threats and provide technical support to operational partners, DNDO's Joint Analysis Center provides information products and technical expertise. For example, the Joint Analysis Center provides geographic information on detectors, situational awareness reports, and other overlays in a geospatial viewer. DNDO's Joint Analysis Center Collaborative Information System facilitates information sharing and provides nuclear alarm adjudication support to operational partners, including those in the maritime environment. This system is connected to the Triage system, maintained by the DOE's National Nuclear Security Administration, which enables seamless transition when national-level adjudication assistance is required.

DNDO's operational partners seek to ensure their readiness to counter the nuclear threat. To this end, DNDO brings to bear a unique "red team" that can challenge fielded capabilities using uncommon nuclear sources and scenarios. DNDO supports maritime partners by conducting overt and covert assessments of operations by intentionally introducing radiation sources and mock devices against deployed defenses to evaluate the performance of fielded technology, training, and protocols. Engagements are conducted through the Area Maritime Security

Committees or directly with the federal, state, or local maritime agency. Recent engagements have included the USCG Maritime Security Response Team and the Florida Wildlife and Conservation Commission.

An act of nuclear terrorism or the interdiction of a nuclear or radiological threat at a U.S. port would necessitate rapid, accurate attribution based on sound scientific evidence. Nuclear forensics, when coupled with intelligence and law enforcement information, supports leadership decisions. DNDO's National Technical Nuclear Forensics Center focuses on developing and improving the readiness of the overarching USG nuclear forensic capabilities, advancing our technical capabilities to perform forensic analyses on pre-detonation nuclear and other radioactive materials, and building and sustaining an expertise pipeline for nuclear forensic scientists. As with its detection mission, DNDO must closely collaborate with interagency partners, particularly those in the FBI, DoD, DOE, and the intelligence community.

The operational readiness of U.S. nuclear forensics capabilities has improved markedly in recent years, as demonstrated by increasingly realistic and complex interagency exercises. Many of the exercises, which were traditionally conducted only by federal partners, now include state and local law enforcement and the intelligence community in order to plan and synchronize the fusion of intelligence, law enforcement, and technical forensics information.

DNDO also supports various efforts to advance technical forensics capabilities related to radiological materials. We have developed, and continue to provide input to, a radiological sealed-source database hosted at Argonne National Laboratory. It is the most comprehensive database of radiological sealed-sources in the world and is used to collect and understand sealed radioactive source design types, production and distribution processes and pathways, and country of origin profiles. The database has been used during operational events by FBI and DOE. DNDO also develops and produces radiological Certified Reference Materials to ensure measurement precision that is sufficient to determine the length of time since the material was last processed.

Our Nation's ports are central to international trade and commerce. An attack on a U.S. seaport with a dirty bomb would cause disruption to the global supply chain, whether directly or indirectly. The collective international efforts to reduce the amount of available material, develop national detection architectures, and deploy detection systems to interdict illicit material, are vitally important in minimizing the risk of a weapon entering the United States. These efforts, coupled with the USG's development and enhancement of domestic defenses present adversaries with multiple obstacles as they seek to attack us using nuclear or other radioactive material. Our national nuclear forensics capabilities will ensure responsible parties are held accountable for their actions. We will continue to work with our partners to counter nuclear terrorism and we sincerely appreciate this Subcommittee's interest in and support for securing the homeland.

Thank you again for this opportunity, and I am happy to answer any questions from the Subcommittee.

TESTIMONY OF

TODD C. OWEN
Assistant Commissioner
Office of Field Operations

U.S. Customs and Border Protection
Department of Homeland Security

BEFORE

U.S. House of Representatives
Committee on Transportation and Infrastructure
Subcommittee on Coast Guard and Maritime Transportation

ON

"Prevention of and Response to the Arrival of a Dirty Bomb at a U.S. Port"

October 27, 2015
Washington, D.C.

Chairman Hunter, Ranking Member Garamendi, and distinguished Members of the Subcommittee, it is an honor to appear before you today to discuss the role of U.S. Customs and Border Protection (CBP) in preventing and responding to radiological weapons-related threats, a role that we share with the Department of Homeland Security (DHS) agencies that join me today.

As the lead DHS agency for border security, CBP works closely with our domestic and international partners to protect the Nation from a variety of dynamic threats, including those posed by containerized cargo and commercial conveyances arriving at our air, land, and sea ports of entry (POE). CBP's security and trade facilitation missions are mutually supportive: by utilizing a risk-based strategy and multilayered security approach, CBP can focus time and resources of those suspect shipments that are high-risk which, in turn, allows CBP to expedite legitimate trade. This approach incorporates three layered elements to improve supply chain integrity, promote economic viability, and increase resilience across the entire global supply chain system:

- *Advance Information and Targeting.* Obtaining information about cargo, vessels, and persons involved early in the shipment process and using advanced targeting techniques to increase domain awareness and assess the risk of all components and factors in the supply chain;

- *Government and Private Sector Collaboration.* Enhancing our Federal and private sector partnerships and collaborating with foreign governments to extend enforcement efforts outward to points earlier in the supply chain; and

- *Advanced Detection Equipment and Technology.* Maintaining robust inspection regimes at our POE, including the use of non-intrusive inspection equipment and radiation detection technologies.

These interrelated elements are part of a comprehensive cargo security strategy that enables CBP to identify and address the potential use of containerized cargo to transport radiological weapons, such as "dirty bombs" or radiological dispersal devices (RDD), before they arrive at our Nation's POE.

Advance Information and Targeting Capabilities

CBP's multilayered approach to cargo security necessitates substantial domain awareness and intelligence to effectively identify and address high-risk shipments. Statutory and regulatory requirements for the submission of advance information, and the development of rigorous targeting capabilities at the National Targeting Center-Cargo, enable CBP to detect potential threats before a vessel or shipment arrives.

The Trade Act of 2002,[1] which provided statutory support for our 24-Hour Advance Cargo Manifest rule, requires importers and carriers to submit, to CBP, advance electronic cargo information for all inbound shipments in all modes of transportation. Furthermore, CBP requires

[1] Pub. L. No. 107–210

the electronic transmission of additional data, as mandated by the Security and Accountability for Every Port (SAFE Port) Act of 2006,[2] through the Importer Security Filing and Additional Carrier Requirements rule (also known as "10+2"). This advance information requirement is a critical element of CBP's targeting efforts at the National Targeting Center-Cargo (NTC-C) and has enhanced CBP's capability to identify high-risk cargo without hindering legitimate trade and commerce.

The NTC-C, established in 2001, coordinates and supports CBP's anti-terrorism activities related to the movement of cargo in all modes of transportation – sea, truck, rail, and air. Using the Automated Targeting System (ATS), NTC-C proactively analyzes advance cargo information before shipments depart foreign ports. ATS incorporates the latest cargo threat intelligence and national targeting rule sets to generate a uniform review of cargo shipments, and provide comprehensive data for the identification of high-risk shipments. ATS is a critical decision support tool for CBP officers working at the NTC-C, the Advanced Targeting Units at our POE, and foreign ports abroad.

Collaboration with Government and Private Sector Partners

CBP's advanced targeting capabilities are further strengthened by our extensive partnerships with other agencies, both domestically and abroad. We work closely with our DHS partners, including the U.S. Coast Guard; U.S. Immigration and Customs Enforcement (ICE); and the Science and Technology Directorate; to coordinate cargo security operations and deploy advanced detection technology. In addition, CBP collaborates with the interagency Domestic Nuclear Detection Office (DNDO) as well as with numerous agencies within the Departments of Defense, Energy, Health and Human Services, Commerce, Justice, and Treasury to promote real-time information sharing. CBP has participated in numerous joint-operations that led to the interdiction of illicit shipments:

- Through Project Synergy, an interagency operation coordinated by DEA's Special Operations Division, NTC-C has identified more than 40 manufacturers in China involved in synthetic stimulant smuggling along with hundreds of U.S. and foreign consignees. This targeting and identification has resulted in significant investigative value to active cases of the Drug Enforcement Administration (DEA) and ICE, as well as providing investigative leads resulting in the creation of new cases. This effort has resulted in a total of 227 arrests, 416 search warrants executed and over $51 million in assets seized.
- Project Zero Latitude was developed due to escalation of foreign and domestic narcotics interceptions involving sea containers of produce and seafood shipments, particularly involving Ecuador. At the NTC-C, CBP conducted an analysis of historical ATS information and cocaine seizure data. The analysis enabled NTC-C to identify several smuggling trends that will facilitate the identification of future suspect shipments.

Close collaboration with our Federal partners increases information sharing, which, in turn, enhances CBP's domain awareness, targeting capabilities, and ability to intercept threats at, or approaching, our borders. CBP continues to extend our cargo security efforts outward through

[2] Pub. L. No. 109-347

strategic partnerships with foreign countries through the development of international cargo security programs and initiatives.

International Partnerships

One of CBP's most effective international cargo security programs is the Container Security Initiative (CSI). This initiative was established in 2002 with the sole purpose of preventing the use of maritime containerized cargo to transport a weapon of mass effect (WME)/weapon of mass destruction (WMD) by ensuring all containers identified as potential risks for terrorism are inspected at foreign ports before they are placed on vessels destined for the United States. Through CSI, CBP officers stationed at CSI ports abroad and the NTC-C work with host countries' customs administrations to identify and mitigate containers that may pose a potential risk for terrorism, based on advance information and strategic intelligence. Those administrations use a variety of means, including detailed data assessment, non-intrusive inspection (NII), radiation detection technology, and/or physical examinations to screen the identified high-risk containers before they depart the foreign port.

CBP works closely with host country counterparts to build their capacity and capability to target and inspect high-risk cargo. Today, in addition to weapons-detection, many CSI ports are now also targeting other illicit materials, including narcotics, pre-cursor chemicals, dual-use technology, stolen vehicles, weapons and ammunition, and counterfeit products. Furthermore, advancements in technology have enabled CBP to increase the efficiency of CSI operations without diminishing effectiveness by conducting more targeting remotely at the NTC-C. CBP's 60 CSI ports in North America, Europe, Asia, Africa, the Middle East, and Latin and Central America currently prescreen over 80 percent of all maritime containerized cargo that is imported into the United States. We anticipate that percentage to increase in the near future. Under a revised Declaration of Principles signed on June 23, 2015, CBP and the General Administration of Customs of the People's Republic of China have agreed to expand their cooperation to address all cargo hazards, increase information sharing and collaboration, and conduct joint inspections in additional ports.

CBP's strong working relationships with our foreign partners are also demonstrated through the Secure Freight Initiative (SFI) in Qasim, Pakistan. Through SFI, all targeting of containers is done remotely by CBP officers working at the NTC-C and physical examinations are conducted at Port Qasim by Pakistani Customs officials and Locally Engaged Staff hired and vetted by the U.S. Consulate General in Karachi. CBP officers use live video feeds streaming directly from Pakistan to the United States to monitor SFI operations at Port Qasim, including physical examinations of containers.

Creating the process for real-time data transmission and analysis required the development, installation and integration of new software and equipment. CBP partnered with the Department of Energy to deploy networks of radiation detection and imaging equipment in Qasim. Port Qasim continues to showcase the SFI program in a country where the government and terminal operators support the initiative, and where construction of dedicated facilities is possible. From constructing the scanning site to providing adequate staffing levels for SFI, the Government of Pakistan remains a strong partner in deploying SFI operations.

All trading nations depend on containerized shipping for the transportation of manufactured goods, which underscores the importance of these two programs. Each year, about 108 million cargo containers are transported through seaports around the world, constituting the most critical component of global trade. Almost 90 percent of the world's manufactured goods move by container, and about 40 percent arrive by ship. Collaboration with foreign counterparts provides increased information sharing and enforcement, further secures the global supply chain, and extends our security efforts outward.

Private-Sector Partnerships

In addition to CBP's targeting capabilities, and our partnerships with Federal and foreign partners, a critical component to CBP's effort to extend our cargo security to the point of origin is our effective partnership with the private industry. CBP works with the trade community through the Customs Trade Partnership Against Terrorism (C-TPAT) program, which is a public–private partnership program wherein members of the trade community volunteer to adopt tighter security measures throughout their international supply chains in exchange for enhanced trade facilitation, such as expedited processing. C-TPAT membership has rigorous security criteria and requires extensive vetting and on-site visits of domestic and foreign facilities. This program has enabled CBP to leverage private sector resources to enhance supply chain security and integrity.

C-TPAT membership has grown from just seven companies in 2001 to more than 11,000 companies today, accounting for more than 54 percent (by value) of goods imported into the United States. The C-TPAT program continues to expand and evolve as CBP works with foreign partners to establish bi-lateral mutual recognition of respective C-TPAT-like programs. Mutual Recognition as a concept is reflected in the World Customs Organization's Framework of Standards to Secure and Facilitate Global Trade, a strategy designed with the support of the United States, which enables Customs Administrations to work together to improve their capability to detect high-risk consignments and expedite the movement of legitimate cargo. These arrangements create a unified and sustainable security posture that can assist in securing and facilitating global cargo trade while promoting end-to-end supply chain security. CBP currently has signed Mutual Recognition Arrangements with New Zealand, the European Union, South Korea, Japan, Jordan, Canada, Taiwan, Israel, Mexico, and Singapore and is continuing to work towards similar recognition with China, Brazil, the Dominican Republic, India and other countries.

Advanced Detection Equipment and Technology

In addition to deploying technology and personnel abroad under programs like CSI, CBP has made strides in strengthening detection equipment capabilities in domestic seaports. Non-Intrusive Inspection (NII) technology enables CBP to detect materials that pose potential nuclear and radiological threats. Technologies deployed to our Nation's land, sea, and air POE include large-scale X-ray and Gamma-ray imaging systems, as well as a variety of portable and handheld technologies. NII technologies are force multipliers that enable us to screen or examine a larger portion of the stream of commercial traffic while facilitating the flow of legitimate cargo.

CBP currently has 307 large-scale NII systems deployed to and in between U.S. POE. These systems enable CBP officers to examine cargo conveyances such as sea containers, commercial

trucks, and rail cars, as well as privately owned vehicles, for the presence of contraband without physically opening or unloading them. This allows CBP to work smarter and faster in detecting contraband and other dangerous materials. To date, CBP has used the deployed NII systems to conduct more than 81 million examinations, resulting in more than18,800 narcotics seizures, with a total weight of more than 5.2 million pounds, and more than $76.2 million in currency seizures.

An integral part of the CBP comprehensive strategy to combat nuclear and radiological terrorism is the scanning of all arriving conveyances and containers with radiation detection equipment prior to release from the POE. In partnership with DNDO, CBP has deployed nuclear and radiological detection equipment, including Radiation Portal Monitors (RPM), Radiation Isotope Identification Devices (RIID), and Personal Radiation Detectors (PRD) has been deployed to 328 POE nationwide.[3] Utilizing RPMs, CBP is able to scan nearly 100 percent of all mail and express consignment mail and parcels; nearly 100 percent of all truck cargo, 100 percent of personally owned vehicles arriving from Canada and Mexico; and nearly 100 percent of all arriving sea-borne containerized cargo for the presence of radiological or nuclear materials. Since the inception of the RPM program in 2002, CBP has scanned more than 1.1 billion conveyances for radiological contraband, resulting in more than 3.3 million alarms, all of which have been successfully adjudicated at the proper level.

When the RPM alarms on a conveyance or package the conveyance or package is referred to secondary inspection. If it is a conveyance, the driver and all passengers are removed from the vehicle. A RIID is then used to determine if the cause of the radiation alarm is due to an isotope used in medical treatments. Otherwise, using the RPM printout page, the CBP officer will complete a 360 degree scan of the conveyance using a RIID. Once the source of the radiation is localized, the officer uses the RIID to identify the radiation isotope. The results are referred for technical analysis through the CBP Laboratories and Scientific Services Directorate Teleforensic Center. All ambiguous RIID results are referred to the Nuclear Regulatory Commission for verification and further action, if necessary.

As part of CBP's NII recapitalization plan, older technology will be phased out and replaced with more modern and state of the art technology. As part of the joint CBP/DNDO Radiation Detection Program Executive Plan, older RPMs will be replaced with more capable technology that is more effective and significantly more efficient. CBP's RIID fleet is in the middle of a major recapitalization. Within the last three years, 27 percent of the RIIDs have been replaced with more precise technology. DNDO has also awarded contracts to replace the remainder over next few years subject to the continued availability of funding.

In conjunction with CBP's many other initiatives (C-TPAT, ATS, NTC-C, 24-Hour Rule, and CSI), NII technology provides CBP with a significant capacity to detect illicit nuclear and radiological materials and other contraband and continues to be a cornerstone of CBP's multilayered cargo security strategy.

---

[3] As of September 30, 2015, CBP currently has 1,281 RPMs, 2,685 RIIDs, and 32,404 PRDs operational systems deployed nationwide.

Response to a Radiological Weapon at a Port

The aforementioned technology, targeting capabilities, and partnerships are strategically aligned to prevent the arrival of a dangerous weapon at a U.S. port. However, in the event such a circumstance occurs, CBP has established contingency plans and standard processes in order to ensure a coordinated and effective response to such an event.

Frontline CBP personnel, upon detection of a suspect radioactive source such as a dirty bomb, are trained to secure, isolate, and notify suspect targets and contact the CBP's Teleforensic Center. The scientists are specially trained in spectroscopy to recognize illicit radiological material and can confer with DOEs Triage Program for additional analysis. Any potential threat information will be referred for immediate action to the Federal Bureau of Investigation's (FBI) Strategic Information Operations Center. The FBI has the lead for the criminal investigation response to a domestic terrorist threat or incident. CBP will coordinate and assist FBI response teams with the investigation of the threat.

CBP's aviation assets maintain an emergency response capability to provide airborne assessment of radiological deposition following a nuclear or radiological accident or incident and provide airborne detection of a lost or stolen radiological source or device. Under an Interagency Agreement with the DOE National Nuclear Security Administration, CBP provides material, supplies, fuel, aircraft, flight crews, ground crews, and other required resources to provide aircraft flight support for the NNSA radiological emergency response mission.

All frontline personnel working at POEs utilize Personal Radiation Detectors (PRD), and receive ongoing training on how to respond to a detected radiological weapon. A dirty bomb uses common explosives to spread radioactive materials over a targeted area. It is not a nuclear blast. The force of the explosion and radioactive contamination will be more localized. While the blast will be immediately obvious, the presence of radiation will not be known until trained personnel with specialized equipment are on the scene. As with any radiation, frontline personnel are trained to limit the risk and effects of exposure by finding a shielding object, increasing their distance from the blast, and minimizing exposure time. Personnel will also work with local HAZMAT to cordon off a perimeter and assist with the decontamination process.

Conclusion

Each year, more than 11 million maritime containers arrive at our Nation's air and seaports. At our land borders, another 11 million arrive by truck and 2.7 million by rail. CBP's targeting activities, in conjunction with programs like CSI and C-TPAT, increase CBP's awareness of what is inside those containers, and enhance our capability to assess whether it poses a risk to the American people.

Working with our DHS, Federal, international, state, local, tribal, and private industry partners, CBP's cargo security programs help to safeguard the Nation's borders and ports from threats – including those posed by radiological weapons.

Chairman Hunter, Ranking Member Garamendi, and distinguished Members of the Subcommittee, thank you for the opportunity to testify today. I would be pleased to answer your questions.

United States Government Accountability Office

GAO

Testimony
Before the Subcommittee on Coast Guard and Maritime Transportation, Committee on Transportation and Infrastructure, House of Representatives

For Release on Delivery
Expected at time, 10:00 a.m.ET
Tuesday, October, 27, 2015

COMBATING NUCLEAR SMUGGLING

Risk-Informed Covert Assessments and Oversight of Corrective Actions Could Strengthen Capabilities at the Border

Statement of David C. Maurer, Director, Homeland Security and Justice

GAO Highlights

Highlights of GAO-16-191T, a testimony before the Subcommittee on Coast Guard and Maritime Transportation, Committee on Transportation and Infrastructure, House of Representatives

Why GAO Did This Study

Preventing terrorists from smuggling nuclear or radiological materials into the United States is a top national priority. To address this threat, DHS has deployed radiation detection equipment and trained staff to use it. CBP conducts covert operations to test capabilities for detecting and interdicting nuclear and radiological materials at air, land, and sea ports of entry into the United States as well as checkpoints.

This testimony addresses the extent to which (1) CBP covert operations assessed capabilities at air, land, and sea ports and checkpoints to detect and interdict nuclear and radiological material smuggled across the border and (2) CBP reported its covert operations results and provided oversight to ensure that corrective actions were implemented.

This statement is based on a September 2014 report (GAO-14-826) and selected updates as of October 2015. In conducting that work, GAO analyzed documents, such as test summaries, directives, and planning and guidance papers and interviewed DHS and CBP officials. We also interviewed officials from the Domestic Nuclear Detection Office (DNDO).

What GAO Recommends

GAO previously recommended DHS use a risk assessment to inform priorities for covert test operations, determine time frames and address barriers for reporting results, and track corrective actions. DHS concurred with the recommendations and reported actions underway to address them. GAO is not making any new recommendations in this testimony.

View GAO-16-191T. For more information, contact David Maurer at (202) 512-8777 or maurerd@gao.gov.

October 27, 2015

COMBATING NUCLEAR SMUGGLING

Risk-Informed Covert Assessments and Oversight of Corrective Actions Could Strengthen Capabilities at the Border

What GAO Found

In its September 2014 report, GAO reported that the Department of Homeland Security (DHS) U.S. Customs and Border Protection's (CBP) Operational Field Testing Division (OFTD) conducted 144 covert operations at 86 locations from fiscal years 2006 through 2013. OFTD selected these locations from a total of 655 U.S. air, land, and sea port facilities; checkpoints; and certain international locations. The results of these operations showed differences in the rates of success for interdicting smuggled nuclear and radiological materials across facility types. OFTD officials stated that the results of its covert operations could be used to assess capabilities at the individual locations tested; but not across all U.S. ports of entry and permanent checkpoints.

GAO also reported that CBP had not conducted a risk assessment to inform and prioritize factors, such as locations, and types of nuclear materials and technologies to be tested in covert operations. CBP had a $1 million budget for covert operations of various activities—including nuclear and radiological testing—from fiscal years 2009 through 2013. Given limited resources, assessing risk to prioritize the most dangerous materials, most vulnerable locations, and most critical equipment for testing through covert operations, could help DHS inform its decisions on how to use its limited resources effectively. DHS agreed with GAO's recommendation to use a risk assessment to inform priorities for covert test operations, but the recommendation remains open. As of October 2015, CBP officials stated that they developed a threat matrix to help determine the sea ports of entry at the highest risk of nuclear and radiological smuggling, but had not completed its assessments for air and land ports of entry.

Finally, GAO reported that OFTD had not issued reports annually as planned on covert operation results and recommendations, which limited CBP oversight for improving capabilities to detect and interdict smuggling at the border. At the time, OFTD had issued three reports on the results of its covert operations at U.S. ports of entry since 2007. However, OFTD officials stated that because of resource constraints, reports had not been timely and did not include the results of covert tests conducted at checkpoints. GAO further reported that OFTD tracked the status of corrective actions taken in response to findings in these reports, but did not track corrective actions identified from their individual covert operations that were not included in these reports. Establishing appropriate time frames and addressing barriers for reporting covert operations results, and developing a mechanism to track all corrective actions would help enhance CBP's accountability for its covert testing and could help inform CBP about further equipment or training required to protect U.S. borders. DHS agreed with GAO recommendations to determine timeframes and address barriers for reporting results, and to track corrective actions; stating that it would address them by April 2015 and December 2014, respectively. As of October 2015, these recommendations remain open as CBP works to fully implement or document actions taken. CBP officials stated they have issued a standard operating procedure containing reporting timeframes, but have not finalized a directive to address this recommendation. GAO is awaiting documentation to demonstrate that CBP is using the database it developed for tracking corrective actions.

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

Chairman Hunter, Ranking Member Garamendi, and Members of the Subcommittee:

I am pleased to be here today to discuss the Department of Homeland Security's (DHS) U.S. Customs and Border Protection's (CBP) covert testing of capabilities to detect and interdict the smuggling of nuclear and radiological materials into the United States. The United States has long faced the threat that terrorists could smuggle nuclear and radiological materials into the United States for use in a potential attack. A terrorist's use of either an improvised nuclear device (IND) or a radiological dispersal devise (RDD)—could have devastating consequences, including not only loss of life, but also enormous psychological and economic impacts. An IND is a crude nuclear bomb that could be immediately lethal to individuals within miles of the explosion, and an RDD—or dirty bomb—would disperse radioactive materials into the environment through an explosive, potentially killing or injuring people within several square miles.

U.S. efforts to counter such threats are considered a top national priority. Since 1995, DHS has invested billions of dollars in equipment and technology, as well as related training for DHS personnel, to better ensure detection and interdiction of smuggled nuclear and radiological materials. Today I will discuss the extent to which (1) CBP covert operations assessed capabilities at air, land, and sea ports and checkpoints to detect and interdict nuclear and radiological materials smuggled across the border and (2) CBP reported its covert operations results and provided oversight to ensure that corrective actions were implemented. My remarks today are based on our September 2014 report findings on these issues and the status of DHS efforts to address related recommendations.[1]

In performing the work for our report, we reviewed planning, policy, and guidance documents, covert operations test summaries and reports showing the number, location, and results of covert operations conducted at U.S. air, land, and sea ports of entry and checkpoints from fiscal year

[1]GAO, *Combating Nuclear Smuggling: Risk-Informed Covert Assessments and Oversight of Corrective Actions Could Strengthen Capabilities at the Border*, GAO-14-826 (Washington, D.C.: September 22, 2014).

2006 through fiscal year 2013. We interviewed agency officials from CBP including the U.S. Border Patrol (USBP), Office of Field Operations (OFO), and the Operational Field Testing Division (OFTD) conducting these operations. We also interviewed officials from the Domestic Nuclear Detection Office (DNDO). More detailed information on the report's scope and methodology can be found in the published report.

The work upon which this testimony is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

CBP has primary responsibility for securing the border against threats to the nation. OFO scans passengers and cargo traveling across the border through U.S. air, land and sea ports of entry to detect and interdict smuggled contraband, including illicit nuclear and radiological materials. USBP conducts inspections for immigration purposes at checkpoints located on roads leading from the border into the United States. OFTD is responsible for conducting covert operations at U.S. ports of entry and checkpoints to test the capabilities for detecting and interdicting nuclear and radiological materials smuggled into the United States, as well as testing capabilities in foreign locations. In selecting sites for covert operations OFTD considered the universe of 655 sites existing at the time of our review. These sites included 477 facilities at 328 ports of entry—which encompassed 241 air, 110 land and 126 sea facilities—35 permanent checkpoints, as well as 143 sites consisting of domestic user fee airports and express consignment carrier facility airports as well as

preclearance locations and Container Security Initiative (CSI) ports in foreign locations.[2]

CBP Screening Process for Nuclear and Radiological Materials

CBP's processes for detecting and interdicting nuclear and radiological material smuggled across the border differ across ports of entry and checkpoints, but consisted of similar functions. At land and sea ports of entry, vehicles or containers entering the United States must first have passed through a Radiation Portal Monitor (RPM) that can detect the presence of neutron- and gamma-emitting radioactive material. If an RPM detected the presence of radioactive material in a scanned container or vehicle, the responding CBP officer was to use a device called a radiation isotope identification device (RIID) to identify the radiation source. For some sources, such as industrial radioactive sources, CBP officers were to contact additional specialized CBP staff to verify the type of source material in question, and if necessary verify the shipper's licensing and other information through the National Law Enforcement Communications Center. At checkpoints and air ports of entry, CBP officers and USBP agents generally relied on devices called personal radiation detectors (PRD), which can detect elevated levels of radiation. Aside from relying on different equipment to detect radiological materials, officers and agents at air ports of entry and checkpoints were to follow the same procedures as those used at sea and land ports of entry.

[2]User fee airports are small airports that have been approved by the Commissioner of CBP to receive, for a fee, the services of a CBP officer for the processing of aircraft entering the United States and their passengers and cargo. Express consignment carrier facilities are separate or shared specialized facilities approved by the port director solely for the examination and release of express consignment shipments. Preclearance is the CBP inspection and clearance of commercial air passengers prior to departure from foreign preclearance locations. CSI locations are selected foreign seaports in which CBP places its officials to determine whether U.S.-bound cargo container shipments from those ports are at risk of containing weapons of mass destruction and illicit drugs. The number of sites can vary depending on how they are counted. For example, depending on the operational needs of the express consignment operator, an express consignment facility can be a hub, which is a separate, unique, single-purpose facility normally operating outside of customs operating hours approved by the port director, or an express consignment carrier facility.

CBP Covert Testing Operations for Detecting and Interdicting Nuclear and Radiological Materials

CBP used covert operations at U.S. ports of entry and checkpoints to test and evaluate whether the systems in place were working as designed to detect and interdict nuclear and radiological smuggling.[3] These operations included an assessment of whether the equipment and technology were working according to specification, the policies and procedures for radiation handling and inspection were adequate to cover various smuggling scenarios, and the extent to which CBP personnel complied with established policies and procedures to detect and interdict nuclear and radiological material smuggled across the border. According to CBP documents, results of covert operations can identify the need for changes in how technology is used to detect nuclear and radiological material, agency policies or procedures, or personnel training to ensure that interdiction programs are working most effectively.[4]

OFTD limited covert operations to the ports of entry and checkpoints where equipment and personnel were permanently placed. According to OFTD officials, CBP did not conduct covert operations outside of the system's current capabilities, or test the system's known vulnerabilities. For example, CBP did not conduct covert operations beyond the technical capabilities and specifications of the RPMs, RIIDs, and PRDs. CBP conducted such tests of equipment capabilities using overt operations.

From 1995 through 2013, CBP invested over $2.5 billion to acquire, deploy, and maintain radiation detection equipment; provide training; and conduct both overt and covert tests of this equipment to assess the equipment's effectiveness. OFTD's budget for covert operations was $1

[3]In response to the Security and Accountability for Every Port Act of 2006, OFTD conducted covert operations to assess the capability to detect and interdict smuggling of nuclear and radiological material at the nation's 22 busiest seaports from fiscal years 2007 through 2008. See 6 U.S.C. § 921. Since that time, CBP determined that additional testing was needed at the border and developed processes to conduct additional covert operations.

[4]CBP also conducts overt operations to test equipment and systems in place to detect nuclear and radiological smuggling.

million for fiscal years 2009 through 2013 to test CBP capabilities in several areas, including radiation and nuclear detection.[5]

Covert Operations Provided Limited Assessments of Capabilities to Detect and Interdict Smuggled Nuclear and Radiological Materials

Covert Operations Assessed Detection and Interdiction Capabilities at Certain Locations and Showed Varying Rates of Success

In September 2014, we reported that OFTD conducted 144 covert operations at 86 locations from fiscal years 2006 through 2013 at air, land, and sea ports of entry, checkpoints, and other sites to assess capabilities to detect and interdict nuclear and radiological material smuggled across the border. Most of OFTD's covert operations were conducted using radiological materials; however, OFTD officials said they conducted one or two tests each year using special nuclear material surrogates (SNM)—radiation test sources with characteristics similar to those of highly enriched uranium or plutonium.

About half of these covert operations were conducted at the southwest border, primarily in the state of Texas. CBP has conducted multiple covert operations within the same states and types of facilities. For example, from 2008 to 2013, CBP conducted 4 operations at Houston's sea ports of entry.

[5]Other areas included document fraud, bioterrorism, canine detection of contraband, agricultural inspections, non-intrusive inspection, and its Trusted Traveler and Immigration Advisory Programs. The $1 million does not include OFTD staff assigned to conduct covert operations. CBP was unable to provide us with a specific breakdown of the funds expended solely for nuclear and radiological covert operations or costs associated with conducting overt operations.

OFTD officials told us that they used three primary factors to determine their site selection for covert operations: (1) volume of traffic and size of the facility, (2) management requests for testing, and (3) follow-up on results of previous covert operations. We found that in selecting locations for covert operations, OFTD considered its universe of 655 sites to include 477 facilities at 328 ports of entry, 35 permanent checkpoints, as well as 143 other sites. OFTD officials stated that the results of its covert operations could be used to assess capabilities at the individual locations tested; however, the results could not be used to assess capabilities across all U.S. ports of entry and permanent checkpoints.

We reported that OFTD test summaries discussing the results of covert operations showed differences across facility types in the rate of success for interdicting smuggled nuclear and radiological materials and reasons for any failure. According to an OFTD official, for a covert operation to be considered successful, a CBP officer or USBP agent has to both detect and interdict the radiation test source in accordance with CBP's Radiation Detection Standard Operating Procedures Directive. Our review of the results of 38 covert operations conducted in fiscal years 2012 and 2013 is available in the sensitive but unclassified version of this report, but has been redacted for the purposes of this public testimony.

Covert Operations May Not Have Sufficiently Accounted for the Most Critical Nuclear Materials, Potential High-Risk Locations, or Key Nuclear and Radiological Detection Technology

We reported in September 2014 that CBP had not conducted a risk assessment that could inform the decision making process for prioritizing the materials, locations, and technologies to be tested through covert operations.

DHS policy requires that components with limited resources make risk-informed decisions. However, OFTD's covert operations may not have sufficiently accounted for using nuclear materials that posed the highest risk to the country, testing capabilities in higher-risk border locations, or testing in locations that used key detection technologies. Specifically:

- The extent to which OFTD's covert operations used varying source materials was limited. Our review found that OFTD may not have given sufficient priority to testing detection capabilities for the most dangerous materials. According to the CBP officials, OFTD had both gamma and neutron radiation sources available; however, DNDO had a broader variety of sources that CBP used when conducting covert operations with DNDO once or twice a year.

- The locations selected for covert testing may not have been sufficiently taken into account. For example, 45 of 144 OFTD covert operations, or 31 percent of all such operations, were conducted at checkpoints. While checkpoints are an important component in the nation's border security infrastructure, they constituted only about 5 percent (35 of 655) of total locations, and were generally situated from 25 to 100 miles from the border.

- CBP use of key detection technologies may not have been sufficiently taken into account. CBP used a mix of technologies across facility types and locations that could reflect significant differences in capabilities and federal investment. However, CBP's methodology for choosing locations was not clearly linked to these differences in capability and federal investment.

DHS's May 2010 Policy for Integrated Risk Management states that components should use risk information and analysis to inform decision making, and we previously reported on the importance of using risk assessments to determine the most pressing security needs and developing strategies to address them.[6] Moreover, CBP's fiscal year 2009 through fiscal year 2014 strategic plan required that programs use a risk-based approach to detect and prevent the entry of hazardous materials, goods, and instruments of terror into the United States, and OFTD's documented site selection process stated that they should consider available intelligence reports and risk assessments.

CBP's January 2013 Integrated Planning Guidance (IPG) for Fiscal Year 2015 through Fiscal Year 2019 included recommendations that CBP integrate risk analysis into all decision making, including a risk assessment for chemical, biological, radiological, and nuclear threats. At the time of our published report, CBP had not yet taken steps toward conducting such a risk assessment or integrating existing risk assessments into its covert testing decisions. Specifically, the IPG

[6]See GAO, *Student and Exchange Visitor Program: DHS Needs to Assess Risks and Strengthen Oversight of Foreign Students with Employment Authorization*, GAO-14-356 (Washington, D.C.: Feb. 27, 2014); *Aviation Safety: Enhanced Oversight and Improved Availability of Risk-Based Data Could Further Improve Safety*, GAO-12-24 (Washington, D.C.: Oct. 5, 2012); *Federal Lands: Adopting a Formal, Risk-Based Approach Could Help Land Management Agencies Better Manage Their Law Enforcement Resources*, GAO-11-144 (Washington, D.C.: Dec. 17, 2010); and *Commercial Vehicle Safety: Risk-Based Approach Needed to Secure the Commercial Vehicle Sector*, GAO-09-85 (Washington, D.C.: Feb. 27, 2009).

included recommendations that CBP conduct an in-depth risk and vulnerability assessment by mode and region to clearly identify the future threats that CBP will be facing to better align resources with priorities. According to OFTD, OFO, and USBP officials, they did not have risk assessments that could be used to help inform covert testing decisions. A DNDO official stated that DNDO has previously assessed the risks of nuclear and radiological smuggling through various entry points to the United States, pursuant to DNDO's responsibilities under the Global Nuclear Detection Architecture (GNDA)—the GNDA is a strategy involving an integrated system of radiation detection equipment and interdiction activities to combat nuclear smuggling in foreign countries, at the U.S. border and inside the United States.[7] DNDO officials told us that they would share information they have with CBP; however CBP officials stated that DNDO's information may not be applicable for OFTD's risk-based site selection process.

We concluded that conducting a risk assessment that identifies priorities could help enable CBP to target the program's efforts to maximize the return on the limited resources available and recommended that CBP conduct or use a risk assessment to inform the department's priorities–related to such decisions such as test, locations, materials, and equipment—for covert operations at U.S. checkpoints and points of entry in air, land, and sea environments. DHS concurred with the recommendation and in its official response, stated that it would formulate a process for conducting or using information from risk assessments to inform its priorities and decisions on selecting test locations, materials, and equipment for covert operations. In October 2015, CBP officials informed us that they worked with other components to develop a threat matrix to help determine the sea ports of entry at the highest risk of nuclear and radiological smuggling, but that CBP had not completed its assessments for air and land ports of entry.

[7]The DHS GNDA Implementation Plan identifies specific DHS-led programs and activities that support the mission, goals, and responsibilities discussed in the GNDA strategic plan.

CBP Could Have Reported More Consistently on Covert Operation Results and Provided Greater Oversight of Corrective Actions

OFTD Covert Test Reports Were Not Timely and Did Not Encompass All Locations where Operations Were Conducted

In September 2014, we reported that OFTD had issued periodic reports on the results of its covert operations but had not met its goal for reporting these results on an annual basis for all locations where operations were conducted. According to a document on OFTD's policies and procedures for follow-up on covert testing, an OFTD goal was to compile and analyze its findings from covert operations at the end of each fiscal year to determine whether results showed trends and systemic weaknesses. To communicate these findings, OFTD's policy stated that its goal was to issue reports to CBP management that included a discussion of the findings and the recommendations necessary to address the identified deficiencies. At the time of our report, OFTD had issued three periodic reports that summarized results from covert operations testing capabilities to detect and interdict nuclear and radiological materials smuggled across the border ports of entry: (1) the Summary Report of OFTD Seaport Assessments for fiscal years 2007 through 2008; (2) the Comprehensive Report on Radiation Testing, which summarized the results of covert operations conducted at air, land, and sea ports of entry from fiscal years 2009 through 2011; and (3) the Comprehensive Report on Radiation Testing, which summarized the results of covert operations conducted at air, land, and sea ports of entry from fiscal years 2012 and 2013. OFTD officials stated that while their intention was produce comprehensive reports on an annual basis, they were unable to do so because of resource constraints.

OFTD officials stated that they had not yet issued a report on results of covert operations conducted at checkpoints and were in the process of developing the report recommendations. OFTD began covert operations to test capabilities at checkpoints in fiscal year 2009, but did not include results of checkpoint covert operations in its Comprehensive Report on Radiation Testing. OFTD officials said that they provided three briefings to CBP senior management in fiscal years 2012 and 2013 on preliminary

findings and recommendations resulting from covert operations at checkpoints conducted from fiscal years 2009 through 2013. OFTD officials said they planned to issue a comprehensive report for checkpoint covert operations for fiscal years 2009 through 2013 by the end of December 2014.

Standards for Internal Control in the Federal Government states that program managers are to receive operational information to help them determine whether they are meeting strategic and performance plans, and that pertinent information is to be identified, captured, and distributed to the right people in sufficient detail, in the right form, and at the appropriate time to enable them to carry out duties and responsibilities efficiently and effectively. Further, these internal controls help managers achieve program objectives by ensuring they receive information on a timely basis to allow effective monitoring, enhancing their ability to address weaknesses.[8]

We concluded that timely reporting of weaknesses identified by covert operations could help CBP management provide timely and necessary oversight to OFO and USBP and appropriately address high-priority border vulnerabilities. We recommended that CBP determine time frames for OFTD reporting of covert operations results and work with OFTD to address any barriers to meeting these time frames. DHS agreed with our recommendation and in its official response, CBP stated that it would develop new policies and procedures to ensure that covert testing results are comprehensive and reported in a timely manner by April 30, 2015. In October 2015, CBP officials informed us that they have issued a standard operating procedure containing reporting timeframes and are working to finalize a directive to address our recommendation.

CBP Provided Limited Oversight to Ensure Implementation of Corrective Actions

In our September 2014 report, we found that OFTD tracked some corrective actions taken by CBP components to address weaknesses identified by covert operations, but not others. For example, OFTD tracked the status of corrective actions taken by OFO management to address recommendations included in its comprehensive reports resulting from covert operations. However, we found that OFTD did not track the

[8]See GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999).

status of corrective actions taken by OFO at ports of entry to address weaknesses identified in covert operations that were not individually cited in these reports. Additionally, OFTD did not track the status of corrective actions taken by USBP to address the weaknesses identified through covert operations at checkpoints.

At the time of our report, OFTD officials told us that in order to develop the recommendations issued in the Comprehensive Reports on Radiation Testing, they reviewed the test summaries from all covert operations at air, land, and sea ports of entry and used their judgment to develop recommendations to address capability weaknesses related to equipment, technology, and personnel compliance with policies and procedures in the CBP radiation detection directive. The fiscal years 2009 to 2011 comprehensive report summarized results from 43 covert operations conducted at air, land, and sea ports of entry, and the fiscal years 2012 and 2013 report summarized results from 26 covert operations. The two comprehensive reports span a 5-year time period, and both identified several of the same issues: (1) CBP officers' noncompliance with radiation detection policies and procedures, (2) radiation detection equipment not always functioning as designed, and (3) CBP officer error primarily due to the lack of training. Our assessment of OFTD's fiscal year 2012 and 2013 report found that it provided CBP senior management with a more detailed analysis of covert operation results, including reasons why test sources were not interdicted, than previous reports.

We found that while OFTD was tracking the status of recommendations from their comprehensive reports, CBP was not tracking the corrective actions taken by ports of entry and checkpoint management to address weaknesses found in their individual covert tests that were not included as recommendations in OFTD's comprehensive reports. According to OFTD officials, immediately following a covert operation, OFTD would provide the results—including the methodology, nuclear and radiological source material used, as well as the weaknesses found—to OFO or USBP management at both the location where the test took place and headquarters. OFO or USBP management was responsible for determining the corrective actions needed and ensuring that the corrective actions were implemented. OFTD officials told us that OFO and USBP management was responsible for determining and implementing the corrective action needed because the cause of the weakness detected could vary. For example, an OFO manager might determine if the weakness was related to the failure of one individual to comply with a radiation detection procedure, or if the weakness was related to the

failure of a procedure affecting overall port operations. Corrective actions would be tailored by the port manager accordingly to address the underlying cause of the weakness. At the time of our report, OFO and USBP officials stated that while they had a process in place to address weaknesses identified during OFTD covert operations, they were unable to provide us with complete information about these corrective actions because they did not fully track them. OFTD officials also informed us that OFTD did not track information about corrective actions taken by OFO and USBP because doing so was outside of OFTD's responsibilities.

Standards for Internal Controls in the Federal Government states that agencies can enhance their ability to address weaknesses by establishing policies and procedures for ensuring that the findings of audits and reviews are promptly resolved, and ensure that ongoing monitoring occurs.[9] We concluded that without an overall mechanism for addressing weaknesses identified, CBP does not have the oversight capabilities necessary to hold officials at ports of entry and checkpoints accountable for managing program operations to detect and interdict transborder nuclear and radiological threats. We recommended that CBP develop a mechanism to track the corrective actions taken to address all weaknesses identified by covert operations at the ports of entry and checkpoints. DHS agreed with our recommendation and in its official response, CBP stated that it would develop and implement a mechanism to monitor the status of corrective actions taken by all operational offices as a result of OFTD's covert testing by December 31, 2014. As of October 2015, CBP's officials had developed a database to track and monitor corrective action plans for post covert radiation testing and we are awaiting confirmation that it is in operation.

Chairman Hunter, Ranking Member Garamendi, and members of the subcommittee, this concludes my prepared statement. I would be happy to respond to any questions you may have.

[9]Specifically, managers are to (1) promptly evaluate findings from audits and other reviews, including those showing deficiencies, and recommendations reported by those who evaluate agencies' operations; (2) determine proper actions in response to findings and recommendations from audits and reviews; and (3) complete, within established time frames, all actions that correct or otherwise resolve the matters brought to management's attention. GAO/AIMD-00.21.3.1.

GAO Contacts and Staff Acknowledgements

If you or your staff members have any questions about this testimony, please contact me at (202) 512-8777 or maurerd@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Other contributors included Cindy Ayers, Nima Patel Edwards, Susan Hsu, Brian Lipman, and Ned Woodward.

GAO's Mission	The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.
Obtaining Copies of GAO Reports and Testimony	The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."
Order by Phone	The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm. Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537. Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.
Connect with GAO	Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts and read The Watchblog. Visit GAO on the web at www.gao.gov.
To Report Fraud, Waste, and Abuse in Federal Programs	Contact: Website: http://www.gao.gov/fraudnet/fraudnet.htm E-mail: fraudnet@gao.gov Automated answering system: (800) 424-5454 or (202) 512-7470
Congressional Relations	Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548
Public Affairs	Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

Remote Detection of Nuclear Material

Dr. Gregory H. Canavan
Senior Fellow Los Alamos

Neutrons have been studied extensively for detection of nuclear materials because they have developed sources; penetrate deeply; and produce strong signatures that penetrate to distant sensors that have undergone extensive development. DOD studies of inspection by beams and sensors at several kilometers led to large beams, detectors, and doses so they were discarded.

Sources and detectors can be automated and moved close to the object interrogated, but thermal systems can be negated by absorbers and moderators. Boron and Cd absorbers reduce thermal flux 10-fold, and a few cm of Carbon reduces neutron energies to thermal where absorbers are most efficient. Together they could reduce the nuclear signal from thermal neutrons to insignificant levels (Fig. 1).

A fast spectrum avoids absorption by remaining above this threshold. The Fermi Age theory used to design fast reactors can keep track of both the source neutrons and those from fissile material, which represent the noise and signal, respectively (App 1). The source energy can be chosen to fit a cargo container or other object of interest. (Fig. 2) The noise and signal neutron currents are widely separated at any time (Fig. 3), so the fraction of noise that scatters into the signal is small (App. 2). The advantage that gives the signal in energy more than offsets its disadvantage in current. That produces high confidence identification of SNM that is insensitive to absorbers (Fig. 4).

Moderators increase the target surface area and neutron source. 10-20 cm Carbon would reduce neutron energy to roughly the absorber threshold. Thicker moderators could

eliminate nuclear signals altogether. However, scattering neutrons from them imprints distinctive energy bands whose spacing carries information on moderator type and number indicates moderator thickness as an indication of intentional concealment.

In summary, compact fast neutron inspection provides high-confidence detection of disseminated nuclear designs, materials, and technologies on the time scale on which they could be integrated to take advantage of the large number of containers entering the U.S. ports. They could be deployed on ships, ports, or at sea to support first line defense of the US against nuclear weapons in a manner consistent with the role of the Coast Guard.

LAYOUT OF SOURCES AND DETECTORS

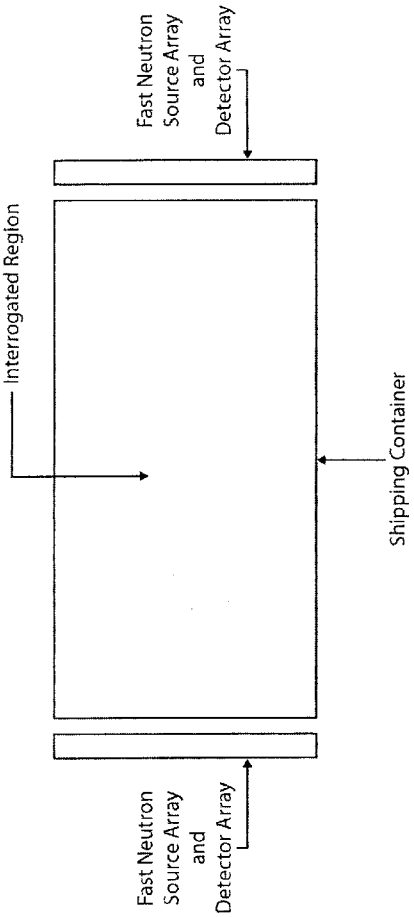


Fig. 1. Scattering & capture lengths

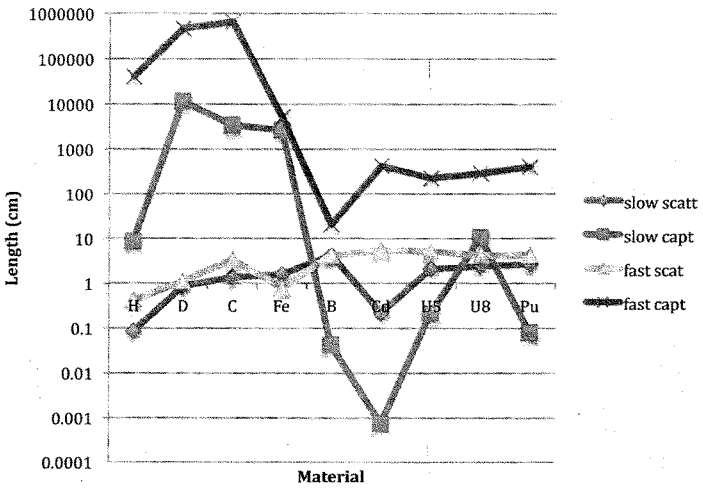


Fig. 2 Source neutrons

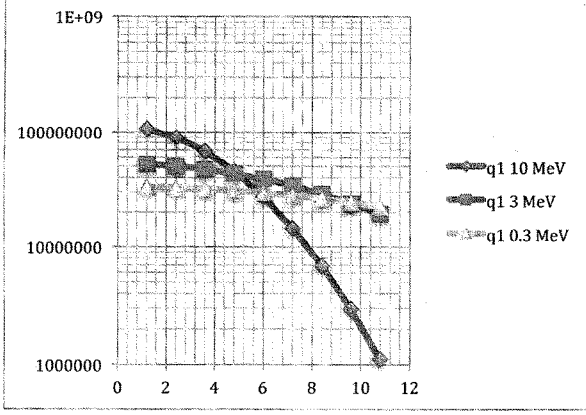


Fig. 2b. Signal neutrons

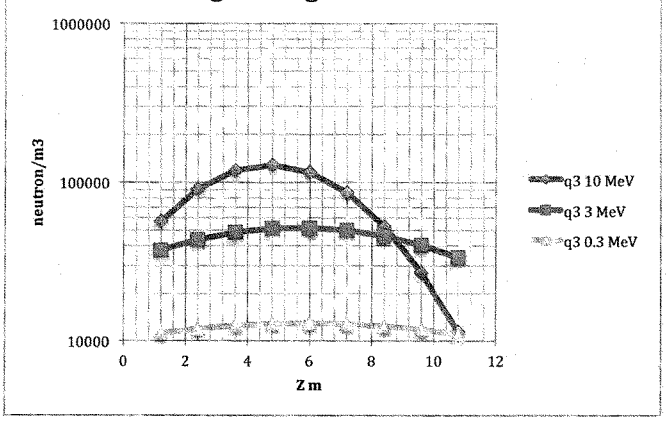


Fig. 3. Slowing time

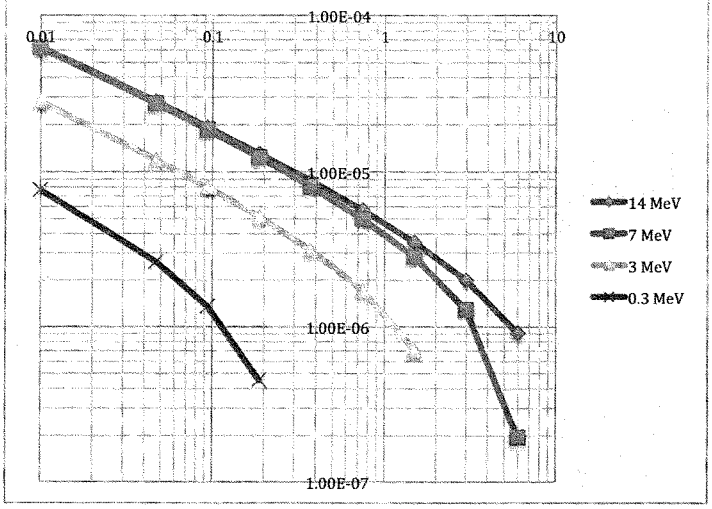
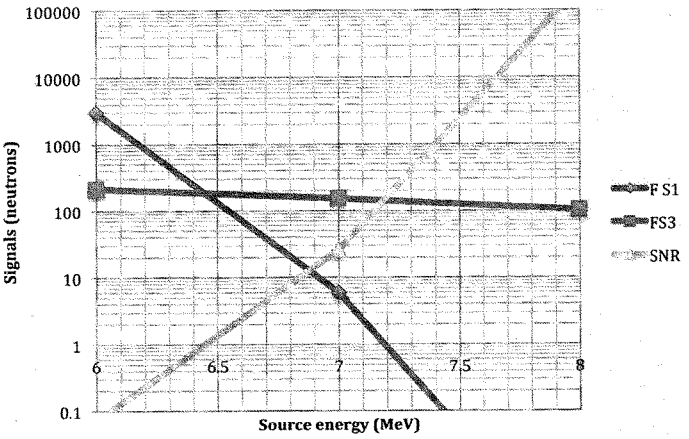


Fig. 4 Signal, noise, and SNR



App. 1. Neutron Diffusion: Fermi Age

- Greens function for a point source Q_3 at r = 0
  - $q_3 = Q_3 G_3 = Q_3 \exp(-r^2/4\tau)/(4\pi\tau)^{3/2}$
- separation variable τ is the Fermi age
  - $\tau = \int d\varepsilon\, \lambda^2/3\xi = (\lambda^2/3\xi)\, \ln(E_o/E)$
- integration over transverse coordinates
  - $q_1 = Q_1 G_1 = Q_1 \exp(-z^2/4\tau)/(4\pi\tau)^{1/2}$
- Source neutrons from array 1-d, follow q_1
- Neutrons scattered from object 3-d, follow q_3

App. 2. Time dependence

- Mean group energy loss rate
  - $dE/dt = (\xi V/\lambda)E$
  - $t = (2\lambda/\xi V_o)(\sqrt{(E_o/E)} - 1)$
  - Same t relates source energy to signal energy
- Number of collisions
  - $N = \ln(Eo/E)/\xi$
- Variance of source distribution
  - $\sigma = 0.33(\xi Eo)^2$ N (Fermi Nuclear Physics)
- Filtering of source neutrons
  - $F1 = 1 - \mathrm{erf}((Esource-Efiss)/\sqrt{(2\sigma)})$

Statement of Charles A. Potter
Distinguished Member of Technical Staff
Domestic Radiological/Nuclear Security and Analysis Department
Sandia National Laboratories

Transportation and Infrastructure Committee
Subcommittee on Coast Guard and Maritime Infrastructure
United States House of Representatives

October 27, 2015

Introduction

Chairman Young, Chairman Hunter, Mr. Larson, and members of the subcommittee, thank you for the opportunity to testify. I am Dr. Charles Potter, a systems analyst and health physicist from Sandia National Laboratories in Albuquerque, New Mexico. Sandia is a multiprogram national security laboratory owned by the United States government and operated by Sandia Corporation for the National Nuclear Security Administration (NNSA). I have come to speak to you today about the current state of the threat of the use of a radiological dispersal device or RDD in the US.

The RDD threat is a very complex and multi-dimensional problem The US government (USG) programs to understand and counter the RDD risk have evolved and matured, and we are gaining a better understanding of how to be effective both domestically and internationally. The science that helps us understand risk has progressed and we at Sandia have been engaged in focused studies that have refined our understanding of some of the specific risks. At this time, we are, at the request of NNSA, just embarking on what is planned to be a multi-participant effort to update and refine our estimates of the potential economic impacts of an RDD attack.

The US government and many of our foreign partners have been working for more than a decade to reduce the risk of a successful RDD attack. "Success" in this context means that an adversary with the intent and the capability manages to acquire the radioactive materials needed, and to launch an attack that results in significant harm, or consequence. The United States government has designed and implemented programs based on scientific studies by Sandia National Laboratories and others to reduce the RDD risk, by reducing the availability and vulnerability of the radioactive materials that could lead to such an attack. This is done by taking an end-to-end systems approach to the problem, looking for those scenarios which

would most likely lead to adversary success, and then reducing the possibility of those scenarios. However, the scientific understanding of the consequences, in terms of cost and methods of cleanup as well as the psychological effects of a successful RDD event, are less well understood and there is currently no single standard on radiation limits for cleanup.

Major Points of This Testimony

- *Terrorist adversaries have shown an interest in RDDs and have attempted to build and use them against targets in the US.As the passage of time allows organizations to gather better understanding of what material is available and how it might be used, this threat may increase.*
- *High-activity radioactive material is common throughout the US and in foreign countries due to its use in medical and industrial applications. In many cases adversaries can find out where these materials are located. The security of high-activity radiation sources during transport is also of concern.*
- *Programs backed by risk analysis and technical study exist throughout the USG to address material security, pathway detection, and threat response. However, much work remains, for example, the development of a capability for disposal of high-activity cesium chloride sources.*
- *Mitigation and long-term recovery has not yet been studied in enough detail to support the development of standards for cleanup, nor the development of large scale decontamination methods. This limits our ability to produce credible cost estimates.*

The Terrorist Threat as Pertaining to RDDs

Al Qaeda publications indicate that the organization considers the main consequences of an RDD attack to be both economic and psychosocial due to the long term effects associated with a quarantine on a high population area and the attendant forced relocation of the public from their homes and businesses. Dhiren Barot in 2006, Jose Padilla in 2007, and Glendon Crawford in August of this year were convicted for attempting to develop and use an RDD in New York City, Chicago, and elsewhere. RDDs can be developed by a spectrum of adversaries, from a relatively low capability "lone wolf," such as these three individuals, to a highly capable and technically competent adversary such as Aum Shinrikyo who perpetrated the coordinated sarin attacks on the Tokyo subway system in 1995. The more technically capable an adversary is, the more likely they would be to find ways to spread the radioactive material over larger areas and at higher radioactivity levels. In addition, as was seen in the World Trade Center attacks in 1993 and 2001, the adversary is adaptive and able to gain knowledge from previous attempts. Obtaining a clear picture of adversary planning is difficult, and it is it is prudent to assume that the necessary motive and intent exists. Our duty then is to ensure that credible scenarios

leading to high-consequence RDD attacks are made as difficult as possible to our potential adversaries.

The report *"Dirty Bombs": Technical Background, Attack Prevention and Response, Issues for Congress*[1] describes the motivation an adversary may have for perpetrating an RDD attack. The immediate results indicated are prompt casualties and panic. Prompt casualties will be caused mainly by the explosion itself. Prompt radiological health effects due to the explosive dispersion of the radioactive material are limited roughly to the explosive damage zone, a few tens of meters from the blast. The explosive consequence may still be significant; consider the effects of the Boston Marathon bombing in 2013. The known presence of radioactive material would only add to the panic and could result in additional casualties from the stress of the situation.[2]

Addionally, the report states that the following four motivations would result in effects felt over an extended period of time following the event, and some would likely affect the entire nation. These would be economic disruption due to the suspension of commerce in the area, area denial or quarantine that could last months or years, decontamination — a high cost endeavor that could result in considerable demolition and long-term casualties from exposure to radioactive material.

Availability of Radiological Material for RDD

In 2008, the report *Radiation Source Use and Replacement*[3] by the National Research Council described the then current use and availability of radiological sources in the US. The report also provided an overview of the risks posed by the malevolent use of the various radioactive materials and made recommendations for alternative technologies, both through use of a radiation generating device instead of a radioactive material source and through non-radiological means. Combined with the general security posture following the September 2001 attacks, this report stimulated USG programs for hardening of radiological devices, enhancing security systems in radiological facilities, and encouraging users to consider changing to technologies that do not require the use of radioactive sources.

The US NRC, through the Title 10 CFR Part 37 regulations on radioactive source security, requires manufacturers and users to have appropriate security controls based on the type and amount of material in use. Security upgrades on cesium chloride blood and research

---

[1] Jonathan Medalia, "Dirty Bombs": Technical Background, Attack Prevention and Response, Issues for Congress. Congressional Research Service, June 14, 2011.
[2] Fukushima stress deaths top 3/11 toll. *The Japan Times.* Feb 20, 2014
[3] National Research Council. Radiation Source Use and Replacement: Abbreviated Version. Washington, DC: National Academies Press, 2008.

irradiators, a considerable concern identified in the report, have been implemented on approximately 60% of irradiators in use in the US and this work is still ongoing.

Past accidents involving cesium-137 indicate extreme difficulty in decontaminating surfaces exposed to this highly chemically active element. Because of the breadth of the liabilities associated with high-activity cesium chloride sources, the 2008 US National Research Council study recommended phase-out of these sources and replacement with lower risk alternatives. In 2008 the USG instead opted for enhanced security of these sources[4] but new developments in alternative technology are making phase out more feasible. For example, France and Norway have enacted legislation aimed at ending the use of cesium chloride irradiators in those countries. Irradiators using cesium chloride sources are located in most of the major US cities and in locations such as hospitals and universities, where a full spectrum security minded culture typically does not exist.

While security at fixed facilities using high-activity radiation sources has been increased by the NRC and enhanced by NNSA for those posing special risks, there is still work to be done in ensuring the sources are equally secured during transport in and through the US. Multiple government agencies (federal, state, and local) are involved in transportation security and more work is needed in harmonizing the security protocols for high-activity radiation sources.

Programs to Address the RDD Threat

Since the 2007 UCLA study on RDD risk at the ports of Los Angeles and Long Beach, many policies, programs, and systems have addressed the threat likelihood. The USG has implemented programs to address both security of materials and pathway interdiction. The DOE's Office of Radiological Security has an extensive program that helps businesses, hospitals, and universities that employ radiological sources considered at risk, to enhance the security of those sources, above the Title 10 Part 37 requirements, and operate in an environment where the risk is reduced. The office also runs the Off-Site Source Recovery Program where unused sources are safely removed and protected. The In-Device Delay Program and other security enhancements focus on preventing and deterring theft of cesium chloride irradiator sources. The Domestic Nuclear Detection Office (DNDO) oversees the Global Nuclear Detection Architecture, a multi-faceted, layered, defense-in-depth framework, with the objective of making the illicit acquisition, fabrication, and transport of a nuclear or radiological device, material, or components prohibitively difficult. DNDO also relies on a well-conceived arrangement of fixed and mobile radiological and nuclear technical detection capabilities to

[4] US Nuclear Regulatory Commission. NRC Staff Recommends Security ofver Replacement of Cesium Chloride Radiation Sources. *NRC News*, 08-223, Dec. 12, 2008.

present terrorists with many obstacles to a successful attack, greatly increasing costs, difficulty, and risk, and thereby deterring them.

If a device is identified prior to detonation, multi-agency response teams are on 24-hour watch and able to respond and interdict quickly. If the worst happens and an RDD is detonated, the multi-agency consequence management function within the USG is there to monitor, treat victims, and make recommendations regarding recovery.

An additional program worthy of mention is *Securing the Cities*, an effort first implemented in New York and currently being expanded to the Los Angeles/Long Beach area. This DNDO program funds the development of area wide security and radiological detection and response capabilities to address the radiological and nuclear threat as well as training and equipping law enforcement and other stakeholders in the area. The program covers all aspects of the threat including material security, pathway interdiction, and target protection. The high-activity sources which could lead to a serious area denial consequence can be detected with existing technologies being used by DHS. This program increases awareness of high risk sources in larger cities and builds programs for fast response to alarms.

There is no current process for disposal of high-activity cesium chloride devices in the US once they are past their useful life. The existing radioactive material waste disposal sites accept only low-level waste designated Class A and Class B, with only a single facility in Texas accepting Class C, the highest activity sources still considered as low-level waste. However, most of the cesium chloride irradiator sources are designated "Greater than Class C," and those that do not fit the generic Class C definition would not likely be accepted by a commercial facility's waste acceptance criteria. Remaining sources become the responsibility of the US government.

Long-Term Recovery from an RDD Event

RDDs are unlikely to result in large immediate health effects beyond those caused by the explosive blast, although there may be some long-term effects to more exposed individuals. However, depending on the radionuclide involved, the economic consequences could be considerable. If the radionuclide is difficult to remove from surfaces, as some are, the contaminated area could be off limits for months or even years. This would result in businesses within those areas being effectively shuttered and residents being relocated semi-permanently or permanently, while costly decontamination efforts are undertaken. Additionally, there would be interdepencies in a quarantined area between the residents and the businesses they patronize. Internationally, there have been three major events causing widespread contamination: the Chernobyl accident in 1986, the spread of contamination from a discarded cesium-137 source in Goiania, Brazil in 1987, and more recently the Fukushima Daiichi disaster in 2011. At Chernobyl and Fukushima, cleanup of the areas is still ongoing and has been a

considerable struggle, albeit those events are larger in area and more contaminated than would be expected from an RDD event. In Goiania, where a relatively small amount of radioactivity was spread by human action, 85 houses were contaminated and 45 public places and 50 vehicles required decontamination. Seven of the houses were demolished because decontamination was not feasible.[5]

Since there is no single US standard for post-cleanup radiation levels, it is difficult to estimate the costs that would be directly associated with decontamination. The Department of Homeland Security in 2006 published their *Protective Action Guides for Radiological Dispersal Device and Improvised Nuclear Device Incidents*[6] which stated:

> Because of the broad range of potential impacts that may occur from RDDs and INDs ranging, for example, from light contamination of a street or building, to widespread destruction of a major metropolitan area, a pre-established numeric guideline was not recommended as best serving the needs of decision makers in the late phase. Rather, a site-specific process is recommended for determining the societal objectives for expected land uses and the options and approaches available to address RDD or IND contamination.

While this philosophy is understandable, a seemingly small decrease in the radiological limit standard for decontamination limits can result in a vastly more expensive and time consuming decontamination.. If this philosophy is retained, it is important to understand the ramifications of cleanup criteria for use in decision-making, but it may be preferable to prepare a technically-based general process and recommendations that could be somewhat tailored to the specific event. At this time, the International Commission on Radiological Protection recommends a residual radiation dose to residents over the long term of 1 mSv/year[7], the National Council on Radiation Protection and Measurements recommends 0.25 mSv/yr[8], and the CERCLA "Superfund" law requires a risk-based evaluation that has resulted in cleanup standards at the Hanford and Rocky Flats DOE sites of 0.15 mSv per year.[9]

A growing trend worldwide is the concept of resilience in cities around the world, and the Rockefeller foundation has recently established the *100 Resilient Cities* initiative that funds the

---

[5] International Atomic Energy Agency. The Radiological Accident in Goiania. Vienna, 1988.
[6] Department of Homeland Security. Protective Action Guides for Radiological Dispersal Device and Improvised Nuclear Device Incidents. *Federal Register* Vol 17(1), 174–196, Jan. 3, 2006.
[7] International Commission on Radiological Protection. Application of the Commission's Recommendations to the Protection of People Living in Long-term Contaminated Areas after a Nuclear Accident or a Radiation Emergency. *Annals of the ICRP* Vol. 39 (3), 2009.
[8] National Council on Radiation Protection and Measurements. Management of Terrorist Events Involving Radioactive Material. Bethesda, MD, NCRP Report No. 138, 2001.
[9] Comprehensive Environmental Response, Compensation, and Liability. Title 42 United States Code Chapter 103.

creation of resilience programs. The vision of the initiative is to encourage cities to prepare for significant disasters through planning and development of response capabilities. A better understanding of the costs and required actions following an RDD attack would provide important considerations for this and similar programs as they prepare for the consequences of an RDD event.

Conclusion

In summary, the RDD risk is real and multi-faceted, and the US government has implemented a number of programs to increase the security of US radiological materials and increase the difficulty of illicit movement of these materials, resulting in a reduced likelihood of an RDD attack. However, there is still significant uncertainty in our understanding of the costs that would accrue after such an event. The development of policies and technical capabilities for effective cleanup to allow for resumption of normal operations following an RDD attack would constitute an important element of the multi-dimensional, integrated solution for addressing the RDD threat.

Thank you.

AAPA American Association of Port Authorities
Alliance of the Ports of Canada, the Caribbean, Latin America and the United States

Seaports Deliver Prosperity

Testimony by Joseph Lawless
Director of Maritime Security
Massachusetts Port Authority
On behalf of the
American Association of Port Authorities (AAPA)

Prevention of and Response to the Arrival of a Dirty Bomb at a U.S. Port

Subcommittee on Coast Guard and Maritime Transportation
Tuesday, October 27, 2015
10:00 a.m.
2167 Rayburn House Office Building

Thank you Chairman Hunter and Ranking Member Garamendi for convening this important and timely hearing. My name is Joseph Lawless. I am the Director of Maritime Security at the Massachusetts Port Authority (MASSPORT) and I am here today on behalf of the American Association of Port Authorities where I am the Chairman of the Security Committee.

AAPA is the unified and collective voice of the seaport industry in the Americas. AAPA empowers port authorities, maritime industry partners and service providers to serve their global customers and create economic and social value for their communities. Our activities, resources and partnerships connect, inform and unify seaport leaders and maritime professionals in all segments of the industry around the western hemisphere. Security is a top priority for all of our members. This testimony is on behalf of our U.S. members.

Securing our ports and communities from dirty bombs cannot happen without strong partnerships. This means the ongoing relationship with port authorities, the federal government, specifically the Customs and Border Protection (CBP), the United States Coast Guard (USCG), the Federal Bureau of Investigation (FBI), shippers, port workers and local law enforcement, who all play a vital role in identifying threats and combining security resources to coordinate if a dirty bomb were to arrive on U.S. shores.

The threat of dirty bombs ending up in the hands of people who want to cause harm to this country, was underscored by accounts of disrupted illicit smuggling operations this fall. It was reported that over the last five years, there have been at least four attempts by criminals in Moldova to sell radioactive materials to Middle Eastern extremists. If any of these smuggling plots were successful, these radioactive materials could be used to

construct a dirty bomb that could ultimately be used against us. The concern is that terrorists could exploit the maritime transportation system to convey a dirty bomb into this country. Stopping dirty bombs before they reach our shores is a priority. But we must have an effective system of detecting dirty bombs if they were to make it to our shores.

A fully funded and staffed Customs and Border Protection Agency is the first step in fighting the threat of dirty bombs. CBP officers meet the ships at all ports of entry to check the manifests and utilize radiation portal monitors.

CBP and ports rely on Radiation Portal Monitors or RPMs to detect dirty bombs in containerized cargo shipped into this country. RPMs are a detection device that provides CBP with a passive, non-intrusive process to screen trucks and other movements of freight for the presence of nuclear and radiological materials. Mandated in the Security and Accountability for Every Port Act (SAFE Port Act) in 2006, the 22 largest container ports by volume must have RPMs and all containers must be screened for radiation.

Almost ten years have passed since RPMs were mandated. However, a decade into this program, questions have been raised regarding who pays for the maintenance of the RPMs, who is responsible for paying for new portals during a port expansion and what is the long term obligation for the next generation of RPMs? A DHS Inspector General 2013 CBP Radiation Portal Monitors at Seaports report states that *"Initial estimates of the deployed RPMs showed an average useful life expectancy of 10 years."*

What we hear repeatedly from our member ports is, the lack of clarity in funding and administering the RPM program, has become a real hindrance in how we protect our ports.

We are fast coming to the end of the first generation of RPMs' life expectancy. Ports such as Tampa, Jacksonville, Long Beach, NY/NJ, and Mobile have all reported complicated discussions with their regional CBP officers on the ongoing responsibilities related to the RPMs.

A recent example is the Port of Jacksonville (JAXPORT) where CBP requested that JAXPORT assume financial responsibility for the RPMs technology sustainment, i.e., hardware, software, and connectivity. This is significant given the complex and critical nature of these federally owned and currently maintained systems.

Other ports are reporting similar disruptions in the RPM program. There is too much at stake for ports and CBP officers to have to engage in policy and funding negotiations. Congress and the Administration must set a clear path on the RPM program.

RPM detection is a federally mandated program. CBP should request adequate federal funding to purchase, install and maintain all RPM equipment at ports throughout the United States. If this is not feasible, then the Department of Homeland Security should

consider the creation a stand-alone priority within the Federal Emergency Management Agency's (FEMA) Port Security Grant Program (PSGP) titled "Radiation Detection Portal Monitors" or expand upon the chemical, biological, radiological, nuclear, and explosives (CBRNE) core capability to allow ports to request security grant funding in support of the purchase and installation of radiation detection portals.

Regarding the PSGP, many port authorities have utilized grants to obtain Rad/Nuc detection equipment. Personal radiation detection devices that first responders wear on their belts, isotope identifiers that are used to determine the sources of radiation alarms and sophisticated backpack detection devices, are some of the items acquired through the PSGP. These items not only supplement CBP's efforts, but also enhance law enforcement's role in the USCG small vessel Rad/Nuc detection program. I would urge Congress to restore funding the PSGP to its original level and maintain the PSGP as a stand-alone Homeland Security Grant Program. Additionally, we would encourage that whenever possible, the grants go directly to the ports, so that our security facilities will have the necessary resources to fully implement their security programs.

In conclusion, we must provide law enforcement agencies, such as CBP and our port security directors, with the tools and the resources to succeed. I appreciate the opportunity to testify this morning and I look forward to answering any questions that you might have.

"A Roadmap for Overcoming the Flaws in the U.S. Government Efforts to Improve Global Supply System Security"

Written Testimony before

a hearing of the

Coast Guard and Maritime Transportation Subcommittee,
Committee on Transportation and Infrastructure,
U.S. House of Representatives

on

Prevention of and Response to the Arrival of a Dirty Bomb at a U.S. Port

by

Stephen E. Flynn, Ph.D.
Professor of Political Science
Director, Center for Resilience Studies
Co-Director, George J. Kostas Research Institute for Homeland Security
Northeastern University
s.flynn@neu.edu

Room 2167
Rayburn House Office Building
Washington, D.C.

10:00 a.m.
October 27, 2015

"A Roadmap for Overcoming the Flaws in the U.S. Government Efforts to Improve Global Supply System Security"

by
Stephen E. Flynn, Ph.D.
Professor of Political Science
Director, Center for Resilience Studies
Co-Director, George J. Kostas Research Institute for Homeland Security
Northeastern University

Chairman Hunter, Ranking Member Garamendi, and distinguished members of the House Coast Guard and Maritime Transportation Subcommittee. Thank you for inviting me to provide testimony on the critically important imperative of preventing and responding to the risk of a dirty bomb in a U.S. port. This marks the 29th time I have appeared as an expert witness before a House or Senate hearing since the attacks of September 11, 2001. Many of these prior hearings also dealt with this complex issue and the enormous stakes that addressing it holds for our economy and national security. It is vitally important that U.S. programs that aim to safeguard the maritime transportation system from the risks associated with weapons proliferation and terrorism continue to receive the oversight this subcommittee is providing today.

Today the subcommittee will hear testimony from Customs and Border Protection, the U.S. Coast Guard, and the Domestic Nuclear Detection Office. You will receive an update on the post-9/11 programs, tools, and protocols whose aim is to prevent terrorists from successfully smuggling nuclear weapons or materials into the United States via the global supply system. To date, the leaders of these agencies have expressed confidence in the strategy and programs they are employing against this risk. In my view, while CBP, USCG, and DNDO deserve good grades for effort, particularly given the complexity of the issue and the relatively modest resources the Bush and Obama Administrations have applied toward it, the threat of a dirty bomb at a U.S. port remains a clear and present danger.

Current U.S. efforts are not up to the task of preventing a determined adversary from exploiting the global supply system and setting off a dirty bomb in a U.S. port. The real threat from such an attack is not the local harm to the port community – as significant as that is likely to be. Instead it is the risk of mass disruption to international commerce that will follow such an attack. A dirty bomb that originates from an overseas source would trigger port closures around the United States that would set off a series of cascading disruptions throughout the global supply system that would lead to billions of dollars of daily losses and cause gridlock across in the intermodal transportation system within 10 days to 2 weeks. Since the U.S. government currently has no comprehensive plan for managing the global recovery of this system in the aftermath of a major security breech, it would almost certainly require several weeks to restore the flow of commerce. This is because it would take time to reassure a traumatized American public so that U.S. ports could be reopened. It would also take time to clear cargo backlogs in transportation hubs and distribution centers around the world, as well as to reposition transportation conveyances so that they can service their normal scheduled routes. The economic impact of such an incident would likely spawn a worldwide recession.

In short, the national security stakes for better managing this risk could not be higher.

The good news is that there is an effective way forward. However, it will require treating this risk with the same kind of urgency and importance that we assign to other major national security challenges. As a stepping off point, the U.S. government needs to shift its emphasis from one that focuses primarily on policing U.S.-bound cargo. Instead it needs to approach the security of the global supply system as a necessary requirement for all nations in meeting their shared international commitments for preventing the proliferation of nuclear weapons and materials and combatting organized crime. Next, it needs to enlist the active participation of the private industry that owns and operates port terminals and transportation conveyances that move supply chains around the planet. There is a business continuity and enterprise resilience imperative associated with the dirty bomb threat that should animate the same kind of close collaboration between the private and public sectors that we saw in the aftermath of the foiled October 2010 cargo planes bomb plot involving explosives hidden in printer cartridges shipped from Yemen. Third, the U.S. government needs to step up efforts to advance the use of new technologies, tools, and protocols on a global scale that can provide for the near real-time visibility and accountability of the contents and location of cargo, thereby bolstering the security and resilience of trade flows. Such a system would be neither too costly, nor difficult to deploy. Based on a study that I have done with my colleagues at the University of Pennsylvania's Wharton School, embedding the capacity within the global supply system to routinely capture non-intrusive images of a container's contents and incorporating them into the data flow that underpins the current risk management process would cost about $15 per container.[1] This is less than the aviation security fee I paid for my domestic flight from Boston to Washington to participate in this hearing.

A CLEAR AND PRESENT DANGER:

The shortcomings of the current U.S. government efforts whose aim is to prevent the kind of scenario that is the subject of today's hearing are well documented by the Government Accountability (GAO) and Congressional Research Service (CRS). My assessment that the nation remains vulnerable to the risk and consequences of a determined adversary targeting a U.S. port with a dirty bomb is based on my 30 years of operational and research experiences in and around the port, transportation, and trade community. This includes my service as a Coast Guard officer from 1982-2002, as the Principal Advisor for the Bi-partisan Congressional Port Security Caucus from 2003-2004, as a member of the National Research Council's Marine Board from 2003-2010, as an independent consultant to major ports and the maritime industry, and currently as a researcher and co-director at the George J. Kostas Research Institute for Homeland Security at Northeastern University.

The three photographs below illustrate the reality that containers can be used as modern-day Trojan horses. Each incident is associated with the most closely regulated segment of the maritime transportation system: the handling of hazardous materials. The first captures the wreckage from a series of explosions that killed 173 people and injured nearly 800 others on

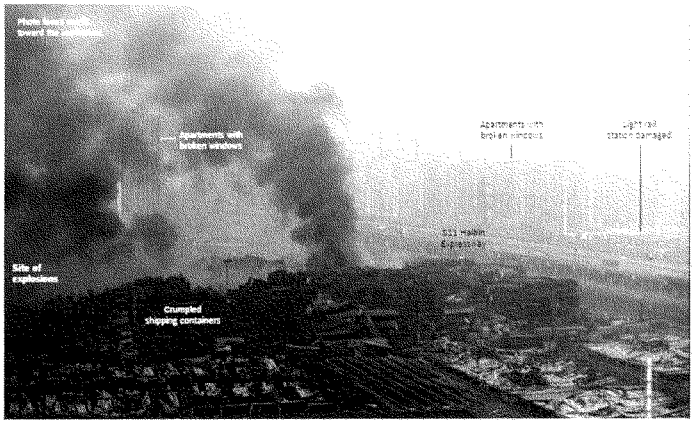
---

[1] Nitin Bakshi, Noah Gans & Stephen Flynn, "Estimating the Operational Impact of Container Inspections at International Ports" *Management Science*, 57:1 (Jan 2011): 1-20.

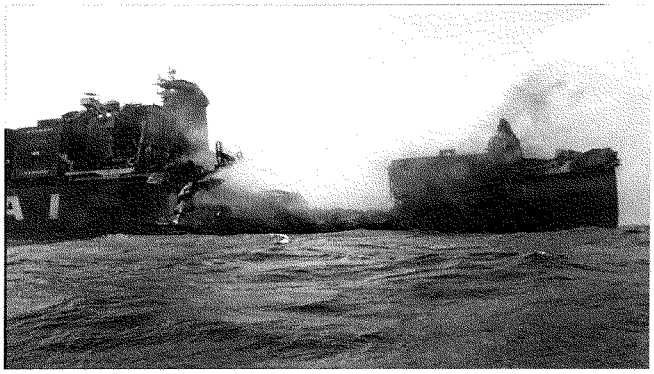
[2] Emma Graham-Harrison, "Huge blasts in Tianjin kill at least 17 and injure hundreds (August 13, 2015) http://www.theguardian.com/world/2015/aug/12/explosion-chinese-port-city-tianjin

[3] Andrew Curry, "Why is this cargo container emitting so much radiation? Wired Magazine (Oct 21, 2011)

August 12, 2015 in the port of Tianjin, China. The explosion occurred at a container storage station within the port. While the cause of the explosions is still under investigation, the Chinese state media reported that the initial blast emanated from unknown hazardous materials that had been loaded in shipping containers stored in a warehouse.[2]

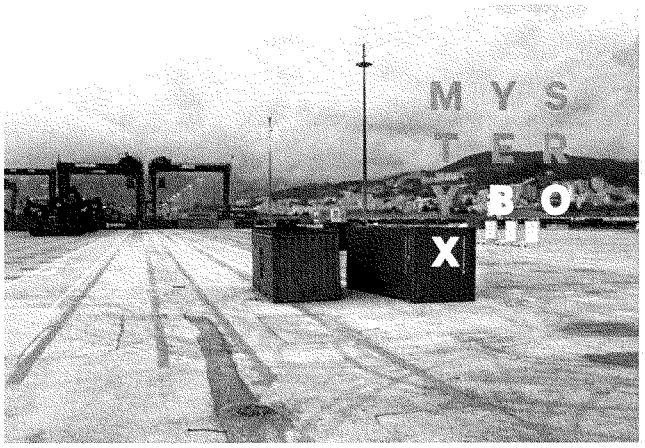


The second is what remains of the M/V Hyundai Fortune after a shipboard explosion off the coast of Yemen on March 21, 2006. No one knows for sure, but the source is assumed to be a containerized shipment of hazardous materials that was not revealed in the cargo manifest that was provided to the ocean carrier. It ended up being stored in a place with inadequate ventilation and ignited, setting off a chain reaction that destroyed this 5,500 TEU container vessel.



[2] Emma Graham-Harrison, "Huge blasts in Tianjin kill at least 17 and injure hundreds (August 13, 2015) http://www.theguardian.com/world/2015/aug/12/explosion-chinese-port-city-tianjin

The third photograph is of a cargo container that arrived in Genoa, Italy on July 13, 2010, emitting Cobalt-60. The source was likely from a medical device or a machine used to sterilize food. Since disposing of this kind of industrial-use radioactive material is very expensive, it was likely placed into the container to simply get rid of it without incurring those costs. The container sat in the port for over a year, as Italian authorities pondered what to do about it. It was finally disposed of on July 29, 2011.[3]



These three incidents reflect the uncomfortable reality that no one really knows what is inside a container except those who are there when the container is packed. This was true before 9/11 and it remains still true today. When it comes to assessing risk, CBP and the Coast Guard must rely on what is represented on the cargo manifest and other shipping documents. But these documents are easily falsified which is why containerized cargo is still used in smuggling every imaginable form of contraband, from narcotics and weapons, to counterfeit goods and currency.

The relative ease at which the global supply system can be compromised by those with nefarious motives can be traced in no small part to its complexity. Figure 1, provides a helpful illustration of this, but this diagram fails to capture the extent to which containerized cargo shipments often originate from multiple factories and involve movements onboard multiple carriers and through multiple ports.

[3] Andrew Curry, "Why is this cargo container emitting so much radiation? Wired Magazine (Oct 21, 2011) http://www.wired.com/2011/10/ff_radioactivecargo/

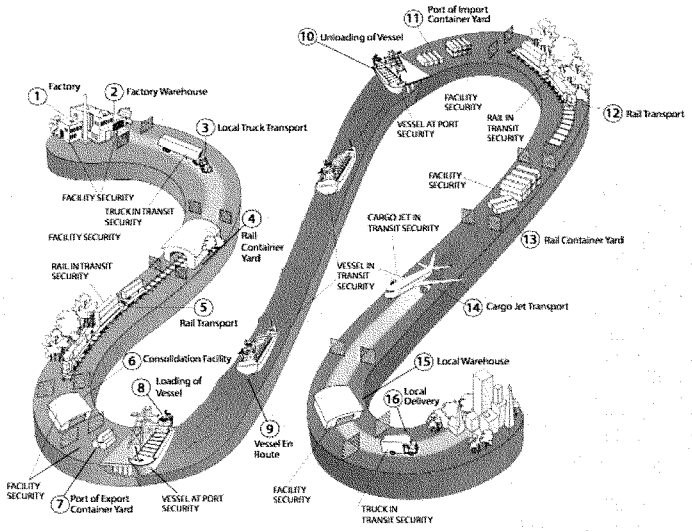


Figure 1: Global supply chains and the intermodal transportation system[4]

THE MORNING-AFTER PROBLEM: THE DISRUPTION OF THE GLOBAL TRADE SYSTEM

If a dirty bomb were set off in a U.S. port, it would not be so much a weapon of mass destruction as it would be one of mass *disruption*. A dirty bomb is a weapon where the kind of industrial grade radioactive material that showed up in a container in Genoa in 2010, is mixed in with conventional explosives. There would be three immediate consequence associated with this attack. First, there would be the local deaths and injuries associate with the blast of the conventional explosives. Second, there would be the environmental damage and extremely high cleanup costs associated with the spread of radioactive material throughout the port infrastructure and the neighboring community. Third, there would be what I have called the "Morning-After Problem": since there would be no way to determine where the compromise to security took place, the entire supply chain and all the transportation nodes and providers must be presumed to present a risk of a potential follow-on attack. Further, all the current U.S. container and port security initiatives would be called into question by such an incident.

On March 28, 2006, nearly a decade ago, I outlined the following hypothetical scenario that had been informed by my own research as well as insights provided by Gary Gilbert who was then chairman of the security committee at Hutchison Port Holdings, the world's largest terminal

[4] *Customs and Border Protection Vision and Strategy 2020* (March 2015): 16. http://www.cbp.gov/sites/default/files/documents/CBP-Vision-Strategy-2020.pdf

operating company. I included it in testimony before the Senate Permanent Subcommittee on Investigations for a hearing on container security:

> A container of athletic footwear for a name brand company is loaded at a manufacturing plant in Surabaya, Indonesia. The container doors are shut and a mechanical seal is put into the door pad-eyes. These designer sneakers are destined for retail stores in malls across America. The container and seal numbers are recorded at the factory. A local truck driver, sympathetic to al Qaeda picks up the container. On the way to the port, he turns into an alleyway and backs up the truck at a nondescript warehouse where a small team of operatives pry loose one of the door hinges to open the container so that they can gain access to the shipment. Some of the sneakers are removed and in their place, the operatives load a dirty bomb wrapped in lead shielding, and they then refasten the door.
>
> The driver takes the container now loaded with a dirty bomb to the port of Surabaya where it is loaded on a coastal feeder ship carrying about 300 containers for the voyage to Jakarta. In Jakarta, the container is transferred to an Inter-Asia ship which typically carry 1200-1500 containers to the port of Singapore or the Port of Hong Kong. In this case, the ships goes to Hong Kong where it is loaded on a super-container ship that carries 5000-8000 containers for the trans-Pacific voyage. The container is then off-loaded in Vancouver, British Columbia. . . . The container is loaded directly from the ship to a Canadian Pacific railcar where it is shipped to a railyard in Chicago. Because the dirty bomb is shielded in lead, the radiation portals currently deployed along the U.S.-Canadian border do not detect it. When the container reaches a distribution center in the Chicago-area, a triggering device attached to the door sets the bomb off.[5]

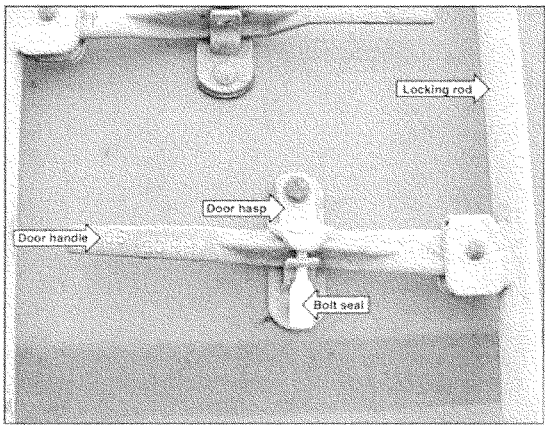
This scenario remains as realistic today as it was in 2006 because it exploits a longstanding vulnerability of the global supply system that still remains unaddressed: the ability of smugglers to potentially target a containerized shipment while it is being transported by a local truck from the factory or logistics center where it originates to the port where it is loaded aboard a vessel. In theory, a manufacturer could direct the trucking firm it uses for local transport to take steps towards assuring the integrity of the shipment in transit. But once a truck leaves a factory, as a practical matter there are few controls in place for preventing a shipment from being diverted before it arrives at a port, particularly if the driver has been recruited, bribed, or intimidated into cooperating with a terrorist group intent on placing a dirty bomb into the container. Container doors are typically "secured" with a numbered bolt seal that can be purchase in volume for as little as $1.50 per bolt. [6] But even if the bolt seal is left in place, the door hinges can be removed or the relatively thin-metal skin of a container can be breeched on the sides or top of the container to gain access to the interior of the box.

---

[5] Stephen Flynn, "The Limitations of the Current U.S. Government Efforts to Secure the Global Supply Chain against Terrorists Smuggling a WMD and a Proposed Way Forward." Hearing on "Neutralizing the Nuclear and Radiological Threat: Securing the Global Supply Chain" before the Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, U.S. Senate, on March 28, 2006.

[6] See American Casting & Manufacturing Association, http://www.seals.com/bolt-locks-blt-1h.asp

Figure 3: A Container Sealed with a Bolt Seal



Source: CBP (photo), GAO (presentation).

Figure 2: Container Sealed with a Bolt Seal

I speculated that the hypothetical terrorist group will purposefully target a container from a "known-shipper" for two reasons. First, it can count on the fact that it is extremely unlikely that CBP will subject that container to any physical scrutiny as it originates from a well-established company that has no past record of being involved in smuggling. Such a shipment from a trusted source would be deemed to be low-risk, and as such not identified for an overseas port-of-loading inspection or an inspection in Vancouver when it is offloaded onto a U.S.-bound train. Second, by exploiting the container from a known-shipper, the terrorist group can be confident that they can generate the maximum amount of fear that all containers previously viewed as "low-risk," will now be judged as potentially presenting a high-risk. Fanned by the inevitable sensational media coverage, governors, mayors, and the American people would place no faith in the entire risk-management regime erected since 9/11. As a result, inbound containers will not be allowed to be offloaded until they are examined. However, there is no way to examine these containers unless they are offloaded. This "Catch-22" will translate into ocean carriers being stranded in anchorages outside ports such as Los Angeles, Oakland, Seattle, Miami, Norfolk, Baltimore, and New York. These delays will then cause back-ups throughout the global intermodal transportation system. Further, there will likely be overwhelming political pressure to enact the 100 percent overseas inspection requirement mandated by "The Implementing Recommendations of the 9/11 Commission Act of 2007", effectively shutting down the flow of commerce to the United States.

Today, the U.S. government still does not have a contingency plan for managing the aftermath of this scenario, even though Congress has mandated that DHS develop one. In June 2007, Secretary Chertoff rolled out "The Strategy to Enhance International Supply Chain Security" that includes a chapter that outlines a response and recovery plan in the aftermath of a major security

incident involving a U.S. port. The plan makes no mention of coordination with overseas port authorities and marine terminal operators, ocean carriers, or even our neighbors in Mexico and Canada. The Obama Administration has not done much better. The *National Strategy for Global Supply Chain Security* issued by the White Hose in January 2012 is a very thin 4 ½ page document that includes the goal of promoting trade resumption policies and practices "that will provide for a coordinated restoration of the movement of goods following a potential disruption." However, it provides no guidance on how that is to be accomplished beyond a call for "developing and implementing national and global guidelines, standards, policies, and programs."[7]

Sixty percent of the world's maritime containers are currently at sea. That translates into 10-12 days of shipping traffic underway in the Pacific Ocean and 8-10 days of traffic in the Atlantic Ocean right now. Many of these container ships are post-Panamax which means that they can only be received at the world's largest 20 seaports and cannot be rerouted. Further, there must be land-based infrastructure to support the offloading and distribution of cargo and that is increasingly concentrated at the major ports. A response and recovery plan that identifies no mechanism to directly engage the global maritime community is not truly a response and recovery plan.

CBP has long recognized the need to work with the private sector. Indeed that is what animated the launching of the Customs-Trade Partnership Against Terrorism (C-TPAT) in the aftermath of 9/11. C-TPAT is a voluntary private-public program that requires participating companies to conduct risk assessments and to complete a supply chain security profile that outlines how they are meeting minimum security criteria. In exchange, participants are promised "reduced inspections at the port of arrival, expedited processing at the border, and other significant benefits, such as "front of the line" inspections and penalty mitigation." According to CBP, as of January 2014, there are 10,650 certified members of C-TPAT that account for 54.1 percent of all imports into the United States. [8]

However, with 10,650 participating companies in C-TPAT, CBP simply lacks the staffing and resources to provide meaningful audits for participating companies to confirm they are being diligent in meeting the relatively minimal security criteria. Given the benefits that go with C-TPAT membership, and the very small odds of being evaluated by CBP for compliance, invariably some companies are tempted to join without making meaningful efforts to bolster their security posture.

CBP emphasizes the importance of embedding risk management into its efforts to secure the global supply chain. As it states in its March 2015 *Vision and Strategy 2020*: "Managing risk at CBP does not preclude adverse events from occurring, but it does enable the Agency to more efficiently focus its resources to address the threat environment."[9] A cornerstone of CBP's risk management approach is the use of advanced sea cargo data provided by

---

[7] The White House, National Strategy for Global Supply Chain Security (January 2012): 3

[8] Customs-Trade Partnership Against Terrorism (C-TPAT) brochure (Revised January 2014) https://www.whitehouse.gov/sites/default/files/national_strategy_for_global_supply_chain_security.pdfhttp://www.cbp.gov/sites/default/files/documents/ctpat_brochure.pdf

[9] *Customs and Border Protection Vision and Strategy 2020* (March 2015): 42. http://www.cbp.gov/sites/default/files/documents/CBP-Vision-Strategy-2020.pdf

importers 24-hours before U.S.-bound cargo is loading in an overseas port. That data is analyzed to assess the extent to which a cargo shipment might pose a high-risk, but this data is essentially based on an honor system. That is it largely assumes that shipping documents are always complete and accurate.

I have long been an advocate of developing measures for securing the global supply chains that emphasize controls that begin where goods originate and having examinations conducted at the port of loading instead of the port of arrival. Shortly after September 11, 2001, I had the opportunity to meet with Robert Bonner, the then Commissioner of U.S. Customs, to discuss a *Foreign Affairs* article I had written in 2000 entitled, "Beyond Border Control." What was to become the Container Security Initiative grew out of those conversations. This approach has the potential to both protect a ship from a HYUNDAI FORTUNE-like incident, as well as safeguard the port where a given container is destined.

Cargo that is deemed suspicious is supposed to be subjected to pre-loading inspections under the Container Security Initiative (CSI) arrangement that is now operating in 58 ports in 30 countries around the world. In 2013, CBP reported that they conducted 103,999 examinations of high-risk cargo in cooperation with their host-country counterparts at the port of loading.[10] Given that there were 11.2 million bills-of-lading, **that number translates into 0.9 percent of U.S. bound cargo or an average of 5 examinations per CSI port per day.**[11] CBP also reported that they subjected 4.1 percent of containers in 2013 to non-intrusive inspection upon arrival in the United States. This translates into only 19 percent of containers that CBP has deemed to be high-risk enough to warrant a closer look, being inspected at the overseas loading port.

There are three reasons why CSI teams are inspecting so little U.S.-bound cargo at the overseas port of loading. First, since the inspections are conducted by the host-country's personnel, CBP has to be careful not to overburden these inspectors with examinations of U.S.-bound cargo that often is done at the expense of these foreign inspectors being able to perform their own work. The overwhelming majority of containers that CBP targets for examination turn out to be benign due to the limits of their targeting algorithm. Requests for lots of examinations that prove to be false alarms endanger the support for CSI by the host country.

The second reason why CBP is so conservative about its port-of-loading requests is that they can be very disruptive to port terminal operations. The decision to examine a container overseas is made after the ocean carrier provides information about that container 24 hours in advance of loading. For larger container ships, that loading process can take 18 hours or more. CBP's decision to have a container inspected before loading ends up placing the shipment at risk of missing its voyage with all the resultant disruption to the importer's supply chain. This is because the container often must be physically removed from the

[10] Vivian C Jones & Lisa Seghetti, U.S. Customs and Border Protection: Trade Facilitation, Enforcement, and Security. Congressional Research Service Report 7-5700 (May 18, 2015): 23. https://www.fas.org/sgp/crs/homesec/R43014.pdf

[11] The arithmetic is straight forward: 103,999 examinations divided by 365 days in the year equals 285 examinations worldwide per day. 285 examinations divided by 58 CSI ports equals an average of 4.9 examinations per port per day.

stacks of containers within the terminal and transported to the inspection facility managed by the overseas customs inspectors. If CBP routinely asked that as little as 1-2 percent of U.S.-bound containers in a major overseas port to be subject to examination before loading, it would likely completely overwhelm the inspection facility.[12] The result would be major delays in shipments. For the overseas marine terminal operator, being directed to routinely locate and remove U.S.-bound boxes from their stacks shortly before scheduled loading can be enormously disruptive to yard operations. These terminals are modern wonders of efficiency. A request to remove a container from their yard is like interrupting a well-honed assembly line.

These challenges associated with conducting CSI examinations at the port of loading translate into the vast majority of containers that CBP deems to be anomalous enough to warrant an inspection, sailing to the United States, and being inspected after they arrive in a U.S. port. CBP has been managing this by essentially creating a two-tier system where only containers it judges to present a very high risk are examined overseas. The problem with this approach is that the targeting system is based almost entirely on anomaly detection and not on specific intelligence. CBP does not have a reliable tool for distinguishing between shipments that are very high risk versus "just" high risk.

Waiting until a container arrives in a U.S.-port before it is examined undermines one of the most important advantages of CSI; i.e., protecting the U.S. port complex and its community from the risks associated with a dirty bomb entering that port. Should a dirty bomb arrive in a U.S. port and be triggered before or during an inspection, it places critical infrastructure and potentially the lives of port workers and the neighboring population at risk. Should it be discovered without being triggered, it will likely shut down port operations for an extended period of time while it is cleared and labor is reassured that it is an isolated incident. Should this be a major port complex such as Los Angeles/Long Beach or Seattle/Tacoma, the resultant disruption to supply chains could reverberate throughout the national economy.

While CBP is largely responsible for container security, the responsibility for overseeing vessel and port facility security rests with the U.S. Coast Guard. The Maritime Transportation and Security Act of 2002 (MTSA) requires that the U.S. Coast Guard assess port security measures within an overseas ports. The Coast Guard uses the International Ship and Port Facility Security (ISPS) Code established by the International Maritime Organization (IMO) in 2004 as the baseline for its assessments. Only vessels transiting from ports deemed to be compliant with ISPS standards are granted access to U.S. ports.

In general, modern port facilities and ocean-going vessels are the most secure segments of the intermodal transportation system. There are limited opportunities for shipments to be compromised once they are inside a container yard both because of the efficiency of maritime terminal operations and the short-staging or "dwell" times for outbound containers. Similarly, containers are so closely stowed on a container ship that once loaded onboard there is no real practical way to gain access to the container door (see figure 3 and figure 4).

---

[12] Nitin Bakshi, Noah Gans & Stephen Flynn, "Estimating the Operational Impact of Container Inspections at International Ports" *Management Science*, 57:1 (Jan 2011): 1-20.

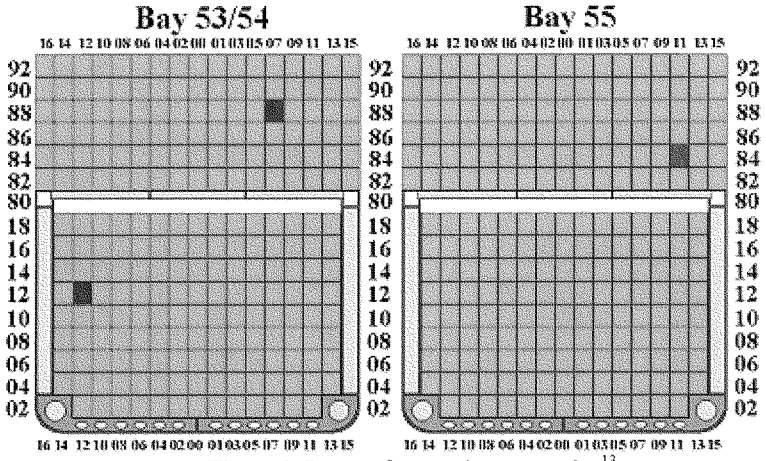


Figure 3: Image of a vessel stowage plan[13]

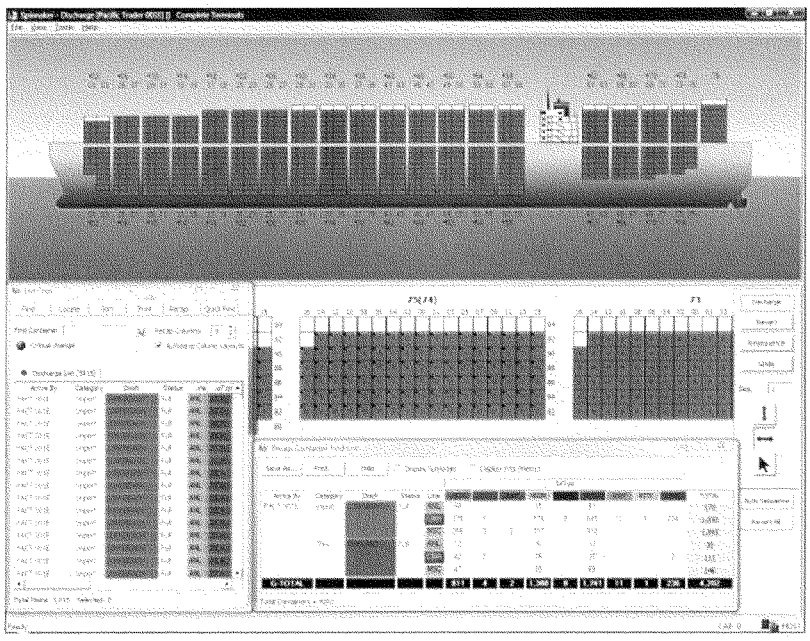


Figure 4: Image of a vessel stowage plan software [14]

[13] Image from http://www.containerhandbuch.de/chb_e/stra/index.html?/chb_e/stra/stra_01_03_03.html

Returning to my hypothetical dirty-bomb scenario, the container originated from a one of the 10,650 companies that now belong to the Customs-Trade Partnership Against Terrorism. It would have transited through multiple ports—Surabaya, Jakarta, Hong Kong, and Vancouver—that have been evaluated by the U.S. Coast Guard as compliant with the International Ship and Port Facility Security (ISPS) Code. Because it came from a trusted shipper, it would not have been identified for special screening by the Container Security Initiative team of inspectors in Hong Kong or Vancouver. Further, since the terrorists placed a lead shield around their dirty bomb, passive radiation portals within these ports or along the U.S.-Canada rail border crossing would be unlikely to detect it.[15] In short, the scenario would end up exposing all the limitations of the current port and container security regime. This would leave the President without a credible basis for authorizing a decision to keep U.S. ports open for trade. Indeed, in the face of a traumatized American public, worried about the possibility of follow-on dirty bomb attacks, the more likely response would be to order the closure of U.S. ports and possibly even U.S. borders until additional security measures can be put in place.

MOVING TOWARDS A MORE SECURE AND RESILIENT GLOBAL SUPPLY SYSTEM

To summarize, should a dirty bomb that originated overseas be set off in a U.S. port, it would represent a major security breech in the global supply system that will trigger U.S. port closures which will, in turn, wreck havoc on international commerce as the intermodal transportation system goes into gridlock. There will be tens of billions of dollars in daily losses, and lives potentially endangered as the shipments of critical time-sensitive goods such as medical supplies and defense-related materials are interrupted. Since the current U.S. container security programs are inadequate for addressing these stakes, the way ahead must involve a far more vigorous effort by the U.S. government to provide incentives for U.S. trade partners and private sector participants to share the responsibility for closely monitoring and validating the international flows of legitimate cargo and to develop robust contingency plans managing security incidents.

STEP 1: The U.S. government needs to shift its emphasis from one that focuses primarily on policing U.S.-bound cargo to one that advancing the overall security and resilience of the global supply system. There is a compelling rationale for taking such an approach: it would help to advance efforts to address the growing risk of WMD proliferation.

---

[14] Image from http://www.shipplanner.com.br/?page_id=102

[15] In the April 2008 issue of *Scientific American*, Thomas Cochran and Matthew McKinzie document what has been long understood by the scientists who understand the physics of radiation detection—that the radiation detectors will only work for unshielded nuclear materials. Since nuclear weapons are shielded by design, they are unlikely to be detected. Highly Enriched Uranium (HEU), the essential ingredient in constructing a nuclear weapon is difficult to detect even in its natural state because it gives off so little radioactivity. As Cochran and McKinzie outline, it requires as little as 1 mm of lead shielding around a canister filled with enough HEU to construct a crude nuclear weapon to avoid detection by the radiation portal technology that DHS has recently deployed within U.S. ports. It would take more lead shielding to avoid detection of a dirty bomb made with commercially-available nuclear materials, but it is likely that a terrorist intent on smuggling such a weapon into the United States would make such an investment. See Thomas B. Cochran and Matthew G. McKinzie, "Detecting Nuclear Smuggling," *Scientific American* (April 2008): 98-104.

The vast majority of the world's cargo and transportation conveyances move amongst nations other than the United States. Ensuring that these shipments are not facilitating the movement of materials and components into the wrong hands is everyone's responsibility. Indeed, UN Security Council Resolution 1540 requires that all nations take actions to detect and intercept outbound shipments of illicit nuclear or radiological materials. The risk is a real one as the Associated Press reported on October 7, 2015. Since 2010, the FBI in partnership with Eastern European authorities, interrupted four attempts by criminal gangs with suspected Russian connections to sell cesium to Middle Eastern extremists. The most recent attempt that was thwarted by authorities reportedly involved enough cesium to contaminate several city blocks and took place in Moldova in February 2015.[16]

STEP 2: The U.S. government needs to enlist the active participation of the private industry that owns and operates port terminals and transportation conveyances that move supply chains around the planet. There is a significant *business continuity* and *enterprise resilience* imperative associated with the dirty bomb threat. As such the conventional wisdom that security within the global transportation and logistics system is more of a public sector responsibility than a private sector one is wrong. The foiled October 2010 bomb plot involving explosives hidden in printer cartridges shipped from Yemen makes the case. In the aftermath of that event, the air cargo industry and U.S. and European authorities closely collaborated on an industry-led effort to more closely scrutinize air cargo before it is loaded on planes.

The maritime transportation system is highly concentrated with just a few large port terminal operators and ocean carriers responsible for handling the vast majority of global cargo. With support from the U.S. government and other authorities, these companies could potentially take on the leadership role for deploying the technologies and tools on a global scale for providing near real-time visibility and accountability of the contents and location of cargo. What they would need is the means to recover the associated costs through a "fee-for-service" requirement borne by importers and exporters. The estimated cost of integrating NII into terminal operations around the world ranges from $3-5 billion.[17] Given the millions of containers moving through those terminals, those costs could be borne by a per-box security surcharge between $10 to $15. Indeed, such a fee-based cost-recovery approach would allow for equipment to be upgraded with new technologies as frequently as every two years.

In 2008, there was an effort by the Port of Los Angeles to work with Hutchison Port Holdings, the largest terminal operator in the world, to develop just this kind of an approach. Specifically, the Port of Los Angeles was interested in finding a way that terminal operators might invest in and maintain NII scanning equipment to examine the contents of containers as they enter their yard. The idea was that if these images could be routinely collected by the

[16] Desmond Butler and Vadim Ghirda, "AP Investigation; Nuclear smugglers sought extremist buyers," AP (October 7, 2015) http://www.msn.com/en-us/news/world/ap-investigation-nuclear-smugglers-sought-extremist-buyers/ar-AAfbV3J

[17] In the interest of full disclosure, since 2011, I have served on the advisory board of Decision Sciences which is a technology company that has developed for commercial use the Multi-Mode Passive Detection System (MMPDS). MMPDS technology was invented by physicists at Los Alamos National Laboratory. It is a passive automated scanning systems for detecting, locating, and identifying unshielded to heavily shielded radiological and nuclear threats.

terminal operator, when government authorities want to examine the contents of a container, these officials could "pull the bits, instead of pulling the box." That is, inspectors could look at the images of the targeted containers collected by the terminal operators. In the vast majority of the cases the images would reveal there is no dense material and therefore there is no risk that the container is carrying a nuclear weapon or shielded material. These containers could then be immediately cleared for loading without their having to be removed from the stacks. Everyone wins. The terminal operator benefits by minimizing the risk of its yard will be disrupted by these inspections. The ocean carrier benefits by having no disruption to its loading plan. The importer benefits by not having the risk that its container will miss the voyage. Finally, CBP benefits by being able to conduct more inspections under the CSI protocol than the current circumstances allow.

Unfortunately, the Port of Los Angeles initiative ran into bureaucratic resistance from CBP. As a result, even though it enjoyed the support of John Meredith, CEO of Hutchison Port Holdings at the time, it ended up being abandoned.

CONCLUSION

The risk of an adversary exploiting the global supply system to import a dirty bomb into a U.S. port and setting it off remains clear and present. The disruption such an attack would generate goes well beyond the local port – it would ripple throughout the maritime transportation system and would be disastrous for global trade. Accordingly, the stakes for U.S. national security and economic security could not be higher. There is an urgent need to significantly bolster and build upon the many post-9/11 initiatives whose aim has been to improve the security of the maritime transportation system. In the end, global networks rely on trust to operate. The private sector must take the lead in developing the systems that sustain that trust. The public sector must be a willing partner in such efforts.

Dr. Stephen Flynn is Professor of Political Science at Northeastern University with faculty affiliations in the Department of Civil and Environmental Engineering and the School of Public Policy and Urban Affairs. At Northeastern, he is also the Founding Director of the Center for Resilience Studies, and Co-Director of the George J. Kostas Research Institute for Homeland Security. Dr. Flynn is also the principal for Stephen E. Flynn Associates LLC, where he provides independent advisory services on improving enterprise resiliency and critical infrastructure assurance, and transportation and maritime security. In addition, he serves on the advisory board of Decision Sciences, a technology company that has developed for commercial use the Multi-Mode Passive Detection System (MMPDS) which is a passive automated scanning systems for detecting, locating, and identifying unshielded to heavily shielded radiological and nuclear threats.

Dr. Flynn is recognized as one of the world's leading experts on transportation security and resilience. In 1991, he began investigating the vulnerability of the intermodal transportation system for exploitation and disruption as both a scholar at the Brookings Institution and as a commissioned officer in the U.S. Coast Guard. Prior to September 11, 2001, he was selected to be an expert advisor to U.S. Commission on National Security (Hart-Rudman

Commission), and following the 9/11 attacks he was the executive director of a blue-ribbon Council on Foreign Relations homeland security task force, again co-led by former Senators Gary Hart and Warren Rudman. In the fall of 2008 he served as the lead homeland security policy adviser for the Presidential Transition Team for President Barack Obama.

Dr. Flynn has been appointed by DHS Secretary Jeh Johnson to serve as a member of the Homeland Security Science and Technology Advisory Council (HSSTAC). He is also a Senior Research Fellow at the Wharton School Risk Management and Decision Processes Center at the University of Pennsylvania and is a member of the National Security Advisory Council for Argonne National Laboratory.

Dr. Flynn has presented congressional testimony before the U.S. Senate and U.S. House of Representatives on 29 occasions since September 11, 2001. From 2003-2004 he served as the Principal Advisor, for the Bi-partisan Congressional Port Security Caucus, U.S. House of Representatives & U.S. Senate. He provided expert advice and comments and recommendations in support of the drafting of the Maritime Transportation Security Act of 2002, the Safe Port Act of 2006, and the 9/11 Recommendations Act of 2007. Dr. Flynn also developed and secured the original funding and legislative support for the post-9/11 Operation Safe Commerce initiative. From 2003-2010 he served as a member of the National Research Council's Marine Board.

Dr. Flynn has traveled extensively abroad where he has investigated transportation security and resilience issues, provided expert advice to government and industry leaders in the ports of Hong Kong, Singapore, Rotterdam, Antwerp, Bremerhaven, Felixstowe, Dubai, Abu Dhabi, Panama, Vancouver, Montreal, and Halifax. He has visited all the major ports in the United States and has been sought out for his expert advice by the Port of Los Angeles, Port Authority of New York/New Jersey, Port of Seattle, Port of Tacoma, Port of Long Beach, Port of Miami, and Port of Baltimore.

He has written numerous articles and two of the most widely-cited books on homeland security The Edge of Disaster: Rebuilding a Resilient Nation (Random House, 2007) and America the Vulnerable (HarperCollins 2004) and frequently advised the Bush Administration on transportation and homeland security issues. Within the Obama Administration he served as a lead-advisor to the Congressionally-mandated Quadrennial Homeland Security Review (QHSR) working group on transportation security, critical infrastructure protection, weapons of mass destruction, and cyber security.

A 1982 graduate of the U.S. Coast Guard Academy, Dr. Flynn served in the Coast Guard on active duty for 20 years, including two tours as commanding officer at sea, received several professional awards including the Legion of Merit, and retired at the rank of Commander. As a Coast Guard officer, he served in the White House Military Office during the George H.W. Bush administration and as a director for Global Issues on the National Security Council staff during the Clinton administration.

He received the M.A.L.D. and Ph.D. degrees from the Fletcher School of Law and Diplomacy, Tufts University, in 1990 and 1991.

○